COMMONWEALTH OF MASSACHUSETTS
ESSEX SUPERIOR COURT

3/14/2022

RECEIVED

MICHAEL ANASTOS, on behalf of himself and all others similarly situated, Plaintiff, v. THE LYON WAUGH AUTO GROUP, Defendant.	Case No. 2277CV00245-A **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff, Michael Anastos, through his attorneys, brings this Class Action Complaint against the Defendant, The Lyon-Waugh Auto Group ("Lyon-Waugh" or "Defendant"), alleging as follows:

INTRODUCTION

1. Lyon-Waugh, a Massachusetts-based car dealership group with over 500 employees, lost control of over 4,300 employees' and customers' highly sensitive personal information in December 2021 in a data breach by cybercriminals ("Data Breach"). On information and belief, cybercriminals were able to access and pilfer Mr. Anastos and Class members' information because Lyon-Waugh fails to maintain adequate cyber security systems, fails to delete unneeded data with sensitive personal information, and fails to train its employees on reasonable security measures, leaving the information an unguarded target for theft and misuse. Mr. Anastos is a former Lyon-Waugh employee and Data Breach victim, asserting this Class Action on behalf of himself and all others harmed by Lyon-Waugh's misconduct.

2. Lyon-Waugh requires that its customers and employees disclose their highly

sensitive personally identifiable information ("PII") to Lyon-Waugh as part of selling its goods and services to customers and providing employment to its employees. Lyon-Waugh, in turn, promises to safeguard that PII using "reasonable physical, electronic and managerial measures to safeguard and secure any information" entrusted to Lyon-Waugh, promising that PII "will be stored in protected databases on secured servers with restricted access[.]"

3. Despite those assurances, in December 2021, cybercriminals hacked Lyon-Waugh's computer systems and accessed PII. Although Lyon-Waugh claims that it "immediately took steps to isolate and secure [its] systems," cybercriminals were able to evade Lyon-Waugh's response long enough to "acquire" PII. Indeed, Lyon-Waugh acknowledges that hackers "stole" PII, including Plaintiff and Class members' names, addresses, dates of birth, Social Security numbers, insurance driver's license numbers and "other benefits information."

4. Despite the devastating nature of the Data Breach, Lyon-Waugh has offered Data Breach victims only 24 months of free credit monitoring services, which does not adequately address the lifelong harm victims will face because of the breach. Indeed, the Data Breach involved Social Security numbers and dates of birth, information that Plaintiff and Class members cannot change and that cybercriminals can misuse to steal their identities.

5. Plaintiff, Mr. Anastos, is a former Lyon-Waugh employee and Data Breach victim. Mr. Anastos brings this Class Action on behalf of himself and all others harmed by Lyon-Waugh's misconduct.

PARTIES

6. Plaintiff, Mr. Anastos, is a natural person and citizen of Massachusetts, residing in Saugus, Massachusetts, where he intends to remain. Mr. Anastos is a former Lyon-Waugh employee and Data Breach victim, receiving Lyon-Waugh's Breach Notice in February 2022.

7. Defendant, "The Lyon-Waugh Auto Group," is the assumed name of an auto group with dealerships throughout Massachusetts, with its principal place of business at 7 Centennial Dr. Peabody, MA 01960. Lyon-Waugh held itself out as a singular entity for purposes of disclosing the Data Breach to the Maine Attorney General's Office[1] but does not appear in Massachusetts' corporate records as an entity. As a result, Plaintiff names "The Lyon-Waugh Auto Group" as a fictitious name under Mass. Gen. Laws ch. 223, § 19 and will amend this Complaint, if necessary, to designate the Defendant's entity name(s).

JURISDICTION & VENUE

8. This Court has subject matter jurisdiction over this action under Gen. Laws ch. 212, § 3.

9. This Court has personal jurisdiction over Lyon-Waugh because Lyon-Waugh is the assumed name for one or more entities doing business and headquartered in the Commonwealth of Massachusetts, such that the entity or entities comprising Lyon-Waugh are "at-home" in this State. Further, the acts or omissions giving rise to this action all took place in Massachusetts.

10. Venue is proper because the acts or omissions from which this action arises all took place in Essex County.

BACKGROUND FACTS

a. Lyon-Waugh

11. Lyon-Waugh is a Massachusetts-based car dealership group with seven locations and 500 employees throughout Massachusetts.

[1] *See* Lyon-Waugh's Data Breach Notification to the Maine Attorney General's Office, https://apps.web.maine.gov/online/aeviewer/ME/40/62ea1496-1f06-4120-aa97-fe1952bd418b.shtml (last visited Mar. 11, 2022).

12. As part of its business, Lyon-Waugh collects sensitive PII from its customers and employees, promising to safeguard that data from theft and misuse using reasonable security measures.

13. Specifically, the PII Lyon-Waugh collects includes names, addresses, dates of birth, Social Security numbers, insurance information, driver's license numbers and "other benefits information."

14. In so doing, Lyon-Waugh recognizes its duty to safeguard PII, promising it "will make every reasonable effort to avoid excessive or irrelevant collection of data," and to "take reasonable physical, electronic and managerial measures to safeguard and secure any information you provide to us (e.g. data will be stored in protected databases on secured servers with restricted access)":[2]

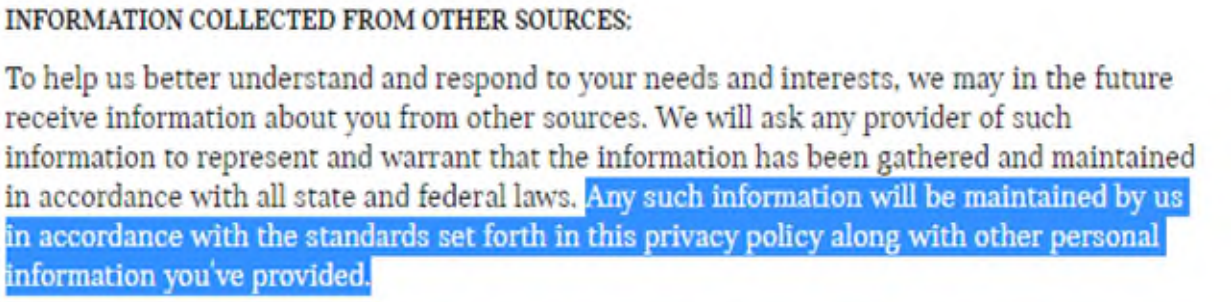
> Our dealership maintains a strict "no-spam" policy. Subscribers to our e-mail services (or any other feature/service found on our Web site) will not receive unsolicited e-mail messages from us. Our dealership collects information online primarily to provide our visitors with a more relevant experience on our sites. When doing so, we will make every reasonable effort to avoid excessive or irrelevant collection of data. Our dealership will take reasonable physical, electronic and managerial measures to safeguard and secure any information you provide to us (e.g. data will be stored in protected databases on secured servers with restricted access). Our dealership will not share any information you've provided to us with anyone without your consent other than to provide the service you've requested. At the time you register for any such service, you will be notified of, and asked to consent to, the sharing of your information with any particular third party necessary to the provision of the requested service.

15. Lyon-Waugh further represents that it "will not share any information you've provided to us with anyone without your consent…"[3]

16. Indeed, Lyon-Waugh's Privacy Policy is clear that its promises to safeguard PII

[2] See Lyon-Waugh's Privacy Policy, https://www.minipeabody.com/privacy.htm (last visited Mar. 7, 2022).
[3] *Id*.

are not limited to those who access its "Web site," but also includes "Information Collected from Other Sources":



INFORMATION COLLECTED FROM OTHER SOURCES:

To help us better understand and respond to your needs and interests, we may in the future receive information about you from other sources. We will ask any provider of such information to represent and warrant that the information has been gathered and maintained in accordance with all state and federal laws. Any such information will be maintained by us in accordance with the standards set forth in this privacy policy along with other personal information you've provided.

17. Despite these assurances, on information and belief, Lyon-Waugh has not implemented reasonable cybersecurity safeguards or policies to protect PII, or trained its employees to prevent, detect, and stop data breaches of Lyon-Waugh's systems. As a result, Lyon-Waugh leaves vulnerabilities for cybercriminals to exploit and give access to PII.

b. Lyon-Waugh Fails to Safeguard PII

18. Plaintiff, Mr. Anastos, is a former Lyon-Waugh employee.

19. As a condition of employment with Lyon-Waugh, Lyon-Waugh requires its employees to disclose their PII.

20. Further, as a condition of buying products and services from Lyon-Waugh, Lyon-Waugh requires its customers to disclose their PII.

21. Lyon-Waugh collects and maintains this PII in its computer systems.

22. In collecting and maintaining the PII, Lyon-Waugh agreed it would safeguard the data according to its internal policies and state and federal law.

23. Still, in or around December 2021, cybercriminals bypassed Lyon-Waugh's cybersecurity safeguards and pilfered the PII stored in Lyon-Waugh's systems.

24. On December 4, 2021, Lyon-Waugh "first learned" of the Data Breach, which "partially disrupted" its information systems. Lyon-Waugh claims it "immediately took steps to

isolate and secure [its] systems," but not before hackers "accessed and acquired certain files from [Lyon-Waugh's] systems, including documents that may have contained [PII.]"

25. In other words, Lyon-Waugh had no effective means to quickly detect, prevent, stop, undo, or remediate the effects of the Data Breach, meaning cybercriminals could easily access and steal PII.

26. After the breach, Lyon-Waugh then "investigate[d]" it to determine how the hack happened and what information was stolen by hackers.

27. But Lyon-Waugh disclosed little from its investigation. Indeed, in its breach notice ("Breach Notice") to victims of the Data Breach, Lyon Waugh did not disclose or was unable to disclose *when* cybercriminals hacked its systems, *how* Lyon-Waugh allowed them to do so, *why* Lyon-Waugh was unable to stop it, and *what* information hackers "acquired." Instead, Lyon-Waugh issued a bare-bones notice informing Data Breach victims that their highly sensitive PII "may be at risk." A true and accurate copy of the Breach Notice is attached as **Exhibit A**.

28. And despite the lifelong harm that Plaintiffs and Class members face, Lyon-Waugh offered them only 24 months of free credit monitoring, which does not adequately address the costs the Data Breach will impose on them.

29. On information and belief, Lyon-Waugh allowed the Data Breach to occur because it failed to adequately train its employees on reasonable cybersecurity protocols or implement reasonable security measures, causing it to lose control over PII. Lyon-Waugh's negligence is evidenced by its failure to prevent the Data Breach and stop cybercriminals from accessing PII. Further, the Breach Notice makes clear that Lyon-Waugh cannot, or will not, determine the full scope of the Data Breach, as it has been unable to determine exactly what

information was stolen and when.

c. Plaintiff's Experience

30. Mr. Anastos is a former Lyon-Waugh employee, working for Lyon-Waugh from approximately 2017 to 2020.

31. As a condition of Mr. Anastos's employment, Lyon-Waugh required Mr. Anastos to provide his PII.

32. Mr. Anastos provided his PII to Lyon-Waugh and trusted that the company would use reasonable measures to protect it according to Lyon-Waugh's internal policies and state and federal law.

33. Mr. Anastos has and will spend considerable time and effort monitoring his accounts to protect himself from additional identity theft. Mr. Anastos fears for his personal financial security and uncertainty over what PII was exposed in the Data Breach. Mr. Anastos has and is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

d. Plaintiff and the Proposed Class Face Significant Risk of Continued Identity Theft

34. Plaintiff and members of the proposed Class have suffered injury from the unauthorized access to, theft, and misuse of their PII that can be directly traced to Defendant.

35. As a result of Lyon-Waugh's failure to prevent the Data Breach, Plaintiff and the proposed Class have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. They have suffered or are at an increased risk of suffering:

a. The loss of the opportunity to control how their PII is used;

b. The diminution in value of their PII;

c. The compromise and continuing publication of their PII;

d. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

e. Lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;

f. Delay in receipt of tax refund monies;

g. Unauthorized use of stolen PII; and

h. The continued risk to their PII, which remains in the possession of defendant and is subject to further breaches so long as defendant fails to undertake the appropriate measures to protect the PII in their possession.

36. Stolen PII is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PII can be worth up to $1,000.00 depending on the type of information obtained.

37. The value of Plaintiff and the proposed Class's PII on the black market is considerable. Stolen PII trades on the black market for years, and criminals frequently post stolen private information openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee of course.

38. In fact, the value of this highly sensitive PII is precisely why hackers targeted and

stole it.

39. It can take victims years to spot identity or PII theft, giving criminals plenty of time to use that information for cash.

40. One such example of criminals using PII for profit is the development of "Fullz" packages.

41. Cyber-criminals can cross-reference multiple sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

42. The development of "Fullz" packages means that stolen PII from the Data Breach can easily be used to link and identify it to Plaintiff and the proposed Class's phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiff and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff and other members of the proposed Class's stolen PII is being misused, and that such misuse is fairly traceable to the Data Breach.

43. Defendant disclosed the PII of Plaintiff and members of the proposed Class for criminals to use in the conduct of criminal activity. Specifically, Defendant opened up, disclosed, and exposed the PII of Plaintiff and members of the proposed Class to people engaged in disruptive and unlawful business practices and tactics, including online account hacking,

unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud), all using the stolen PII.

44. Defendant's failure to properly notify Plaintiff and members of the proposed Class of the Data Breach exacerbated Plaintiff and members of the proposed Class's injury by depriving them of the earliest ability to take appropriate measures to protect their PII and take other necessary steps to mitigate the harm caused by the Data Breach.

CLASS ACTION ALLEGATIONS

45. Plaintiff sues on behalf of himself and the proposed Class ("Class"), defined as follows:

> All citizens of the Commonwealth of Massachusetts whose PII was compromised in the Data Breach disclosed by Lyon-Waugh in its Breach Notice.

Excluded from the Class are Defendant, its agents, affiliates, parents, subsidiaries, any entity in which Defendant has a controlling interest, any Defendant officer or director, any successor or assign, and any Judge who adjudicates this case, including their staff and immediate family.

46. Plaintiff reserves the right to amend the class definition.

47. This action satisfies the numerosity, commonality, typicality, and adequacy requirements under Mass. R. Civ. P. 23.

a. **Numerosity**. Plaintiff is representative of the proposed Class, consisting of approximately 4,300 members, far too many to join in a single action;

b. **Typicality**. Plaintiff's claims are typical of Class member's claims as each arises from the same Data Breach, the same alleged violations by Defendant, and the same unreasonable manner of notifying individuals about the Data Breach.

c. **Adequacy**. Plaintiff will fairly and adequately protect the proposed Class's interests. His interests do not conflict with Class members' interests and he has

retained counsel experienced in complex class action litigation and data privacy to prosecute this action on the Class's behalf, including as lead counsel.

d. **Commonality**. Plaintiff and the Class's claims raise predominantly common fact and legal questions that a class wide proceeding can answer for all Class members. Indeed, it will be necessary to answer the following questions:

i. Whether Defendant had a duty to use reasonable care in safeguarding Plaintiff's and the Class's PII;

ii. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

iii. Whether Defendant was negligent in maintaining, protecting, and securing PII;

iv. Whether Defendant breached contract promises to safeguard Plaintiff's and the Class's PII;

v. Whether Defendant took reasonable measures to determine the extent of the Data Breach after discovering it;

vi. Whether Defendant's Breach Notice was reasonable;

vii. Whether the Data Breach caused Plaintiff and the Class injuries;

viii. What the proper damages measure is; and

ix. Whether Plaintiff and the Class are entitled to damages, treble damages, or injunctive relief.

48. Further, common questions of law and fact predominate over any individualized questions, and a class action is superior to individual litigation or any other available method to

fairly and efficiently adjudicate the controversy. The damages available to individual class members are insufficient to make individual lawsuits economically feasible.

COUNT I
Negligence
(On Behalf of Plaintiff and the Class)

49. Plaintiff realleges all previous paragraphs as if fully set forth below.

50. Plaintiff and members of the Class entrusted their PII to Defendant. Defendant owed to Plaintiff and other members of the Class a duty to exercise reasonable care in handling and using the PII in its care and custody, including implementing industry-standard security procedures sufficient to reasonably protect the information from the Data Breach, theft, and unauthorized use that came to pass, and to promptly detect attempts at unauthorized access.

51. Defendant owed a duty of care to Plaintiff and members of the Class because it was foreseeable that Defendant's failure to adequately safeguard their PII in accordance with state-of-the-art industry standards concerning data security would result in the compromise of that PII—just like the Data Breach that ultimately came to pass. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiff's and members of the Class's PII by disclosing and providing access to this information to third parties and by failing to properly supervise both the way the PII was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

52. Defendant owed to Plaintiff and members of the Class a duty to notify them within a reasonable timeframe of any breach to the security of their PII. Defendant also owed a duty to timely and accurately disclose to Plaintiff and members of the Class the scope, nature, and occurrence of the Data Breach. This duty is required and necessary for Plaintiff and members of the Class to take appropriate measures to protect their PII, to be vigilant in the face

of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

53. Defendant owed these duties to Plaintiff and members of the Class because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew or should have known would suffer injury-in-fact from Defendant's inadequate security protocols. Defendant actively sought and obtained Plaintiff' and members of the Class's personal information and PII.

54. The risk that unauthorized persons would attempt to gain access to the PII and misuse it was foreseeable. Given that Defendant holds vast amounts of PII, it was inevitable that unauthorized individuals would attempt to access Defendant's databases containing the PII—whether by malware or otherwise.

55. PII is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the PII of Plaintiff and members of the Class and the importance of exercising reasonable care in handling it.

56. Defendant breached its duties by failing to exercise reasonable care in supervising its agents, contractors, vendors, and suppliers, and in handling and securing the personal information and PII of Plaintiff and members of the Class which actually and proximately caused the Data Breach and Plaintiff and members of the Class's injury. Defendant further breached its duties by failing to provide reasonably timely notice of the Data Breach to Plaintiff and members of the Class, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiff's and members of the Class's injuries-in-fact. As a direct and traceable result of Defendant's negligence and/or negligent supervision, Plaintiff and members of the Class have suffered or will suffer damages, including monetary damages, increased risk of future

harm, embarrassment, humiliation, frustration, and emotional distress.

57. Defendant's negligence actually and proximately caused Plaintiff and members of the Class actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their PII by criminals, improper disclosure of their PII, lost benefit of their bargain, lost value of their PII, 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.

COUNT II
Invasion of Privacy, Mass. Gen. Laws. Ch. 214 § 1B
(On Behalf of Plaintiff and the Class)

58. Plaintiff and members of the Class incorporate the above allegations as if fully set forth herein.

59. Defendant publicized private details and facts not generally known to the public, not publicly available, and not of legitimate public concern about Plaintiff and Class members by disclosing and exposing Plaintiff's and Class members' PII to enough people that it is reasonably likely those facts will become known to the public at large, including without limitation on the dark web and elsewhere.

60. Plaintiff's and Class members' PII, which included their names, addresses, dates of birth, Social Security numbers, insurance driver's license numbers and "other benefits information," was private and intimate.

61. Defendant's disclosure of the PII unreasonably, substantially and seriously interfered with Plaintiff's and Class members' privacy such that it offends ordinary sensibilities. Defendant should appreciate that the cyber-criminals who stole the PII would further sell and disclose the PII as they are doing. That the original disclosure is devastating to Plaintiff and

Class members even though it may have originally only been made to one person or a limited number of cybercriminals does not render it any less a disclosure to the public-at-large.

62. The tort of public disclosure of private facts is recognized in Massachusetts under Mass. Gen Laws Ch. 214. Plaintiff's and Class members' private PII was publicly disclosed by Defendant in the Data Breach with reckless disregard for the reasonable offensiveness of the disclosure. Such disclosure is highly offensive and would be to any person of ordinary sensibilities. Defendant knew and knows that Plaintiff's and Class members' PII is not a matter of legitimate public concern.

63. As a direct and proximate result of Defendant's conduct, Plaintiff and Class members have been injured and are entitled to damages.

COUNT III
Breach of an Implied Contract
(On Behalf of Plaintiff and the Class)

64. Plaintiff and members of the Class incorporate the above allegations as if fully set forth herein.

65. Defendant offered Plaintiff and members of the Class employment, products, and/or services in exchange for their PII.

66. In turn, and through internal policies, Defendant agreed it would not disclose the PII it collects to unauthorized persons. Defendant also promised to safeguard the PII entrusted to it.

67. Plaintiff and the members of the Class accepted Defendant's offer by providing PII to Defendant in exchange for employment with Defendant and purchasing products and services from Defendant.

68. Implicit in the parties' agreements was that Defendant would provide Plaintiff and

members of the Class with prompt and adequate notice of all unauthorized access and/or theft of their PII.

69. Plaintiff and the members of the Class would not have entrusted their PII to Defendant in the absence of such agreement with Defendant.

70. Defendant materially breached the contract(s) it had entered with Plaintiff and members of the Class by failing to safeguard such information and failing to notify them promptly of the intrusion into its computer systems that compromised such information. Defendant further breached the implied contracts with Plaintiff and members of the Class by:

a. Failing to properly safeguard and protect Plaintiff and members of the Class's PII;

b. Failing to comply with industry standards as well as legal obligations that are necessarily incorporated into the parties' agreement; and

c. Failing to ensure the confidentiality and integrity of electronic PII that Defendant created, received, maintained, and transmitted.

71. The damages sustained by Plaintiff and members of the Class as described above were the direct and proximate result of Defendant's material breaches of its agreement(s).

72. Plaintiff and members of the Class have performed as required under the relevant agreements, or such performance was waived by the conduct of Defendant.

73. The covenant of good faith and fair dealing is an element of every contract. All such contracts impose upon 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 in

addition to its form.

74. 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.

75. Defendant failed to protect the privacy of the PII entrusted to it even though it knew or should have known that Plaintiff and Class members reasonably understood that Defendant would protect such PII and would not have entrusted Defendant with their PII if they had known Defendant would not adequately protect it.

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

77. In these and other ways, Defendant violated its duty of good faith and fair dealing.

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

COUNT IV
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

79. Plaintiff and members of the Class incorporate the above allegations as if fully set forth herein.

80. This claim is pleaded in the alternative to the breach of implied contractual duty claim.

81. Plaintiff and members of the Class conferred a benefit upon Defendant in the form of services through employment and through purchases of Defendant's products and services.

82. Defendant appreciated or had knowledge of the benefits conferred upon itself by Plaintiff and members of the Class. Defendant also benefited from the receipt of Plaintiff and members of the Class's PII, as this was used to facilitate their employment and purchase of products and services.

83. Plaintiff and Class members reasonably understood that Defendant would adequately protect the PII entrusted to it. Plaintiff and the proposed Class would not have provided their PII, purchased Defendant's products and services, or worked for Defendant at the payrates they did had they known Defendant would not adequately protect their PII.

84. Under principals of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiff and the proposed Class's services, payments, and their PII because Defendant failed to adequately protect their PII.

85. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiff and members of the Class all unlawful or inequitable proceeds received by it because of its misconduct and Data Breach.

PRAYER FOR RELIEF

Plaintiff and members of the Class demand a jury trial on all claims so triable and request that the Court enter an order:

A. Certifying this case as a class action on behalf of Plaintiff and the proposed Class, appointing Plaintiff as class representative, and appointing his counsel to represent the Class;

B. Awarding declaratory and other equitable relief as is necessary to protect the interests of Plaintiff and the Class;

C. Awarding injunctive relief as is necessary to protect the interests of Plaintiff and the Class;

D. Enjoining Defendant from further deceptive practices and making untrue statements about its data security practices and capabilities, the Data Breach and the stolen PII;

E. Awarding Plaintiff and the Class damages that include applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;

F. Awarding restitution and damages to Plaintiff and the Class in an amount to be determined at trial;

G. Awarding attorneys' fees and costs, as allowed by law;

H. Awarding prejudgment and post-judgment interest, as provided by law;

I. Granting Plaintiff and the Class leave to amend this complaint to conform to the evidence produced at trial; and

J. Granting such other or further relief as may be appropriate under the circumstances.

JURY DEMAND

Plaintiff demands a trial by jury on all issues so triable.

RESPECTFULLY SUBMITTED AND DATED this 14th day of March, 2022.

/s/ Michael S. Appel
Michael S. Appel, BBO #543898
SUGARMAN, ROGERS, BARSHAK
& COHEN, P.C.
101 Merrimac Street, 9th Floor
Boston, MA 02114
Telephone: (617) 227-3030
appel@sugarmanrogers.com

Lynn A. Toops (to be admitted *pro hac vice*)
COHEN & MALAD, LLP
One Indiana Square, Suite 1400
Indianapolis, IN 46204
Telephone: (317) 636-6481
ltoops@cohenandmalad.com

J. Gerard Stranch, IV (to be admitted *pro hac vice*)
Peter J. Jannace (to be admitted *pro hac vice*)
BRANSTETTER, STRANCH
& JENNINGS, PLLC
223 Rosa L. Parks Avenue, Suite 200
Nashville, TN 37203
Tel: (615) 254-8801
gerards@bsjfirm.com
peterj@bsjfirm.com

Samuel J. Strauss (to be admitted *pro hac vice*)
Raina C. Borrelli (to be admitted *pro hac vice*)
TURKE & STRAUSS LLP
613 Williamson Street Suite 201
Madison, WI 53703
Telephone: (608) 237-1775
Facsimile: (608) 509-4423
Sam@tukerstrauss.com

EXHIBIT A

The Lyon Waugh Auto Group

10300 SW Greenburg Rd. Suite 570
Portland, OR 97223

1-833-903-3648

Or Visit:
https://app.idx.us/account-creation/protect
Enrollment Code: <<XXXXXXXX>>

To Enroll, Please Call:

<<To the Family of>><<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

<<Date>>

Notice of Data Incident

Dear <<Family of>><<First Name>> <<Last Name>>,

What Happened

We are writing to inform you of an incident that may have affected your personal information.

As you may be aware, on December 4, 2021, we first learned of a cyberattack that partially disrupted Lyon Waugh's information systems. Upon learning of the incident, we immediately took steps to isolate and secure our systems and investigate the incident. We retained a third-party forensics firm and a third-party IT managed services firm to secure our systems, remediate any risks, and methodically bring our systems back online. As part of the investigation, on January 7, 2022, we determined that an unauthorized malicious actor accessed and acquired certain files from our systems, including documents that may have contained some of your personal information. Since then, we have been analyzing impacted files to understand what personal information may be at risk, and working to provide notice to individuals and authorities, as applicable.

What Information Was Involved

The type of information differs from individual to individual, but may have included your name, address, date of birth, Social Security number, insurance and other benefits information. You may be receiving this letter as the spouse or dependent of an employee or former employee of The Lyon Waugh Auto Group.

What We Are Doing

Upon learning of the incident, we engaged a well-known forensic investigation firm to identify the scope of the incident and to assist us with securing our systems and data. We have carefully brought our systems back online and we continue to closely monitor our network and information systems for unusual activity. We have also engaged a third-party managed IT services firm to assist us with the restoration of our systems and additional resources. We will continue to further improve security across our company networks and protect from unauthorized access or similar criminal activity in the future.

In addition, we are offering identity theft protection services through IDX, the data breach and recovery services expert. IDX identity protection services include: 24 months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised. To receive credit services, you must be over the age of 18, have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file. If you do not have a credit file, you will not be able to register for credit monitoring services, but you will receive CyberScan monitoring, insurance, and the fully managed identity recovery services from IDX.

What You Can Do

We encourage you to contact IDX with any questions and to enroll in free identity protection services by calling 1-833-903-3648 or going to https://app.idx.us/account-creation/protect and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 6 am - 6 pm Pacific Time. Please note the deadline to enroll is [Enrollment Deadline].

At this time, we have not received any reports that personal information has been subject to fraudulent activity. However, we encourage you to take full advantage of this service offering. IDX representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

For More Information

You will find detailed instructions for enrollment on the enclosed Additional Important Information document. Also, you will need to reference the enrollment code at the top of this letter when calling or enrolling online, so please do not discard this letter.

Please call 1-833-903-3648 or go to https://app.idx.us/account-creation/protect for assistance or for any additional questions you may have.

Sincerely,

Warren Waugh, Jr.

Warren Waugh, Jr.
Managing Partner
The Lyon Waugh Auto Group

(Enclosure)

Additional Important Information

1. **Website and Enrollment.** Go to https://app.idx.us/account-creation/protect and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

3. Telephone. Contact IDX at 1-833-903-3648 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

4. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

5. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting
1-866-349-5191
P.O. Box 105069
Atlanta, GA 30348-5069
www.equifax.com

Experian Fraud Reporting
1-888-397-3742
P.O. Box 9554
Allen, TX 75013
www.experian.com

TransUnion Fraud Reporting
1-800-680-7289
P.O. Box 2000
Chester, PA 19022-2000
www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.
Please Note: No one is allowed to place a fraud alert on your credit report except you.

6. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

To place a security freeze on your credit report, you must send a written request to each of the three major consumer credit reporting agencies by regular, certified, or overnight mail at the addresses below or, if available, comply with the consumer credit reporting agencies 'online security freeze request procedures:

Equifax Security Freeze	Experian Security Freeze	TransUnion Security Freeze
1-888-298-0045	1-888-397-3742	1-888-909-8872
www.equifax.com	www.experian.com	www.transunion.com
P.O. Box 105788	P.O. Box 9554	P.O. Box 160
Atlanta, GA 30348	Allen, TX 75013	Woodlyn, PA 19094

In order to request a security freeze, you may need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past 5 years, provide the addresses where you have lived over the prior 5 years;
5. Proof of current address such as a current utility bill or telephone bill;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

The credit reporting agencies have 3 business days after receiving your request to place a security freeze on your credit report. The credit reporting agencies must also send written confirmation to your within 5 days and provide you with a unique personal identification number (PIN) or password, or both, that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual to access your credit report, you must call or send a written request to the credit reporting agencies by mail, or, if available, comply with the credit reporting agencies' online procedures for lifting a security freeze and provide proper identification (name, address, and Social Security number), and the PIN or password provided to you when you placed the security freeze, as well as the identities of those entities or individuals you would like to receive your credit report, or the specific period of time you want the credit report available. The credit reporting agencies have 3 business days after receipt of your request to lift the security freeze as requested.

To remove the security freeze, you must send a written request to each of the credit reporting agencies by mail or, if available, comply with the credit reporting agencies 'online procedures for removing a security freeze. The credit reporting agencies have 3 business days after receipt of your request to remove the security freeze.

7. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

Masssachusetts Residents: Under Massachusetts law, you have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

Massachusetts law also allows consumers to place a security freeze on their credit reports. See **Section 6** for information on how to place a security freeze on your credit report.

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400. There were ___ Rhode Island residents impacted.

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.

25963

The Lyon Waugh Group

10300 SW Greenburg Rd. Suite 570
Portland, OR 97223

1-833-903-3648

Or Visit:
https://app.idx.us/account-creation/protect
Enrollment Code: <<XXXXXXXX>>

To Enroll, Please Call:

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

<<Date>>

Notice of Data Incident

Dear <<First Name>> <<Last Name>>,

What Happened

We are writing to inform you of an incident that may have affected your personal information.

On December 4, 2021, we first learned of a cyberattack that partially disrupted Lyon Waugh's information systems. Upon learning of the incident, we immediately took steps to isolate and secure our systems and investigate the incident. We retained a third-party forensics firm and a third-party IT managed services firm to secure our systems, remediate any risks, and methodically bring our systems back online. As part of the investigation, on or about January 7, 2022, we determined that an unauthorized malicious actor accessed and stole certain files from our systems, including documents that may have contained some of your personal information. Since then, we have been analyzing impacted files to understand what personal information may be at risk, identify affected individuals and obtain contact information, and working to provide notice to individuals and authorities, as applicable. We have not been made aware of any reports of fraudulent use of personal information as a result of the incident, but wanted to provide you with information about the incident and steps you can take as a precaution.

What Information Was Involved

The type of information included the following contact information about you: <<name, address, social security number, and driver's license>><<name, address, and social security number>><<name, address, and driver's license>>. No payment or other financial information was included.

What We Are Doing

Immediately upon learning of the incident, we engaged a well-known forensic investigation firm to identify the scope of the incident and to assist us with securing our systems and data. We have informed the appropriate authorities, including law enforcement and regulators, as appropriate. We have carefully brought our systems back online and we continue to closely monitor our network and information systems for unusual activity. We have also engaged a third-party managed IT services firm to assist us with the restoration of our systems and additional resources. We will continue to further improve security across our company networks and protect from unauthorized access or similar criminal activity in the future.

In addition, we are offering identity theft protection services through IDX, the data breach and recovery services expert. IDX identity protection services include: 24 months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

What You Can Do

We encourage you to contact IDX with any questions and to enroll in free identity protection services by calling 1-833-903-3648 or going to https://app.idx.us/account-creation/protect and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 6 am - 6 pm Pacific Time. Please note the deadline to enroll is [Enrollment Deadline].

At this time, we have not received any reports that personal information has been subject to fraudulent activity. However, we encourage you to take full advantage of this service offering. IDX representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

For More Information

You will find detailed instructions for enrollment on the enclosed Additional Important Information document. Also, you will need to reference the enrollment code at the top of this letter when calling or enrolling online, so please do not discard this letter.

Please call 1-833-903-3648 or go to https://app.idx.us/account-creation/protect for assistance or for any additional questions you may have.

Sincerely,

Warren Waugh, Jr.

Warren Waugh, Jr.
Managing Partner
The Lyon Waugh Auto Group

(Enclosure)

Additional Important Information

1. **Website and Enrollment.** Go to https://app.idx.us/account-creation/protect and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

3. Telephone. Contact IDX at 1-833-903-3648 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

4. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

5. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting
1-866-349-5191
P.O. Box 105069
Atlanta, GA 30348-5069
www.equifax.com

Experian Fraud Reporting
1-888-397-3742
P.O. Box 9554
Allen, TX 75013
www.experian.com

TransUnion Fraud Reporting
1-800-680-7289
P.O. Box 2000
Chester, PA 19022-2000
www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.
Please Note: No one is allowed to place a fraud alert on your credit report except you.

6. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

To place a security freeze on your credit report, you must send a written request to each of the three major consumer credit reporting agencies by regular, certified, or overnight mail at the addresses below or, if available, comply with the consumer credit reporting agencies 'online security freeze request procedures:

Equifax Security Freeze	Experian Security Freeze	TransUnion Security Freeze
1-888-298-0045	1-888-397-3742	1-888-909-8872
www.equifax.com	www.experian.com	www.transunion.com
P.O. Box 105788	P.O. Box 9554	P.O. Box 160
Atlanta, GA 30348	Allen, TX 75013	Woodlyn, PA 19094

In order to request a security freeze, you may need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past 5 years, provide the addresses where you have lived over the prior 5 years;
5. Proof of current address such as a current utility bill or telephone bill;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

The credit reporting agencies have 3 business days after receiving your request to place a security freeze on your credit report. The credit reporting agencies must also send written confirmation to your within 5 days and provide you with a unique personal identification number (PIN) or password, or both, that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual to access your credit report, you must call or send a written request to the credit reporting agencies by mail, or, if available, comply with the credit reporting agencies' online procedures for lifting a security freeze and provide proper identification (name, address, and Social Security number), and the PIN or password provided to you when you placed the security freeze, as well as the identities of those entities or individuals you would like to receive your credit report, or the specific period of time you want the credit report available. The credit reporting agencies have 3 business days after receipt of your request to lift the security freeze as requested.

To remove the security freeze, you must send a written request to each of the credit reporting agencies by mail or, if available, comply with the credit reporting agencies 'online procedures for removing a security freeze. The credit reporting agencies have 3 business days after receipt of your request to remove the security freeze.

7. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

Masssachusetts Residents: Under Massachusetts law, you have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

Massachusetts law also allows consumers to place a security freeze on their credit reports. See **Section 6** for information on how to place a security freeze on your credit report.

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400. There were ___ Rhode Island residents impacted by the incident.

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.

The Lyon Waugh Group

10300 SW Greenburg Rd. Suite 570
Portland, OR 97223

1-833-903-3648

Or Visit:
https://app.idx.us/account-creation/protect
Enrollment Code: <<XXXXXXXX>>

To Enroll, Please Call:

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

<<Date>>

Notice of Data Incident

Dear <<First Name>> <<Last Name>>,

What Happened

We are writing to inform you of an incident that may have affected your personal information.

On December 4, 2021, we first learned of a cyberattack that partially disrupted Lyon Waugh's information systems. Upon learning of the incident, we immediately took steps to isolate and secure our systems and investigate the incident. We retained a third-party forensics firm and a third-party IT managed services firm to secure our systems, remediate any risks, and methodically bring our systems back online. As part of the investigation, on or about January 7, 2022, we determined that an unauthorized malicious actor accessed and stole certain files from our systems, including documents that may have contained some of your personal information. Since then, we have been analyzing impacted files to understand what personal information may be at risk, identify affected individuals and obtain contact information, and working to provide notice to individuals and authorities, as applicable. We have not been made aware of any reports of fraudulent use of personal information as a result of the incident, but wanted to provide you with information about the incident and steps you can take as a precaution.

What Information Was Involved

The type of information included the following contact information about you: <<name, address, social security number, and driver's license>><<name, address, and social security number>><<name, address, and driver's license>>. No payment or other financial information was included.

What We Are Doing

Immediately upon learning of the incident, we engaged a well-known forensic investigation firm to identify the scope of the incident and to assist us with securing our systems and data. We have informed the appropriate authorities, including law enforcement and regulators, as appropriate. We have carefully brought our systems back online and we continue to closely monitor our network and information systems for unusual activity. We have also engaged a third-party managed IT services firm to assist us with the restoration of our systems and additional resources. We will continue to further improve security across our company networks and protect from unauthorized access or similar criminal activity in the future.

In addition, we are offering identity theft protection services through IDX, the data breach and recovery services expert. IDX identity protection services include: 24 months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

What You Can Do

We encourage you to contact IDX with any questions and to enroll in free identity protection services by calling 1-833-903-3648 or going to https://app.idx.us/account-creation/protect and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 6 am - 6 pm Pacific Time. Please note the deadline to enroll is [Enrollment Deadline].

At this time, we have not received any reports that personal information has been subject to fraudulent activity. However, we encourage you to take full advantage of this service offering. IDX representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

For More Information

You will find detailed instructions for enrollment on the enclosed Additional Important Information document. Also, you will need to reference the enrollment code at the top of this letter when calling or enrolling online, so please do not discard this letter.

Please call 1-833-903-3648 or go to https://app.idx.us/account-creation/protect for assistance or for any additional questions you may have.

Sincerely,

Warren Waugh, Jr.

Warren Waugh, Jr.
Managing Partner
The Lyon Waugh Auto Group

(Enclosure)

Additional Important Information

1. **Website and Enrollment.** Go to https://app.idx.us/account-creation/protect and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

3. Telephone. Contact IDX at 1-833-903-3648 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

4. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

5. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting
1-866-349-5191
P.O. Box 105069
Atlanta, GA 30348-5069
www.equifax.com

Experian Fraud Reporting
1-888-397-3742
P.O. Box 9554
Allen, TX 75013
www.experian.com

TransUnion Fraud Reporting
1-800-680-7289
P.O. Box 2000
Chester, PA 19022-2000
www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.
Please Note: No one is allowed to place a fraud alert on your credit report except you.

6. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

To place a security freeze on your credit report, you must send a written request to each of the three major consumer credit reporting agencies by regular, certified, or overnight mail at the addresses below or, if available, comply with the consumer credit reporting agencies 'online security freeze request procedures:

Equifax Security Freeze	Experian Security Freeze	TransUnion Security Freeze
1-888-298-0045	1-888-397-3742	1-888-909-8872
www.equifax.com	www.experian.com	www.transunion.com
P.O. Box 105788	P.O. Box 9554	P.O. Box 160
Atlanta, GA 30348	Allen, TX 75013	Woodlyn, PA 19094

In order to request a security freeze, you may need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past 5 years, provide the addresses where you have lived over the prior 5 years;
5. Proof of current address such as a current utility bill or telephone bill;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

The credit reporting agencies have 3 business days after receiving your request to place a security freeze on your credit report. The credit reporting agencies must also send written confirmation to your within 5 days and provide you with a unique personal identification number (PIN) or password, or both, that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual to access your credit report, you must call or send a written request to the credit reporting agencies by mail, or, if available, comply with the credit reporting agencies' online procedures for lifting a security freeze and provide proper identification (name, address, and Social Security number), and the PIN or password provided to you when you placed the security freeze, as well as the identities of those entities or individuals you would like to receive your credit report, or the specific period of time you want the credit report available. The credit reporting agencies have 3 business days after receipt of your request to lift the security freeze as requested.

To remove the security freeze, you must send a written request to each of the credit reporting agencies by mail or, if available, comply with the credit reporting agencies 'online procedures for removing a security freeze. The credit reporting agencies have 3 business days after receipt of your request to remove the security freeze.

7. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

Masssachusetts Residents: Under Massachusetts law, you have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

Massachusetts law also allows consumers to place a security freeze on their credit reports. See **Section 6** for information on how to place a security freeze on your credit report.

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400. There were ___ Rhode Island residents impacted by the incident.

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.