UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF TEXAS
DALLAS DIVISION

Nicholas Gorman, on behalf of himself and all others similarly situated, Plaintiff, v. Ethos Group, Inc. Defendant.	Case No.: 3:22-cv-2898 **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Nicholas Gorman ("Plaintiff") brings this Class Action Complaint ("Complaint") against Defendant Ethos Group, Inc. ("Ethos" or "Defendant") as an individual and on behalf of all others similarly situated, and alleges, upon personal knowledge as to his own actions and his counsels' investigation, and upon information and belief as to all other matters, as follows:

I. NATURE OF THE ACTION

1. Plaintiff brings this Complaint against Defendant for its failure to properly secure and safeguard the personally identifiable information that it collected and maintained as part of its regular business practices including, but not limited to, names and driver's license numbers (collectively defined herein as "PII" or "Private Information").

2. Defendant Ethos is a business that provides "financing and servicing of automobiles" to its clients—partner automotive dealers.[1]

[1] https://www.ethosgroup.com/

3. Upon information and belief, former and current customers at automotive dealerships, which are or were partnered with Defendant, were required to entrust Defendant, either directly or indirectly, with an extensive amount of their PII, used for Defendant's business, in order to obtain automobile financing and/or other services from Defendant. Defendant retains this information for at least many years.

4. On August 1, 2022, Defendant became aware of suspicious activity on its networks. Defendant proceeded to investigate the nature and scope of the suspicious activity and subsequently concluded that "some consumer information was accessed between July 30, 2022 and July 31, 2022", including Plaintiff's and Class Members' PII (the "Data Breach").[2]

5. According to Defendant's Notice of Security Incident letter (the "Notice Letter"), the compromised information included individuals' names and driver's license numbers.[3]

6. Defendant's investigation concluded that the PII compromised in the Data Breach included Plaintiff's and approximately 822,000 other individuals' PII.[4]

7. By obtaining, collecting, using, and deriving a benefit from the PII of Plaintiff and Class Members, Defendant assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion.

8. Defendant failed to adequately protect Plaintiff's and Class Members PII —and failed to even encrypt or redact this highly sensitive information. This unencrypted, unredacted PII was compromised due to Defendant's negligent and/or careless acts and omissions and its utter failure to protect customers' sensitive data. Hackers targeted and obtained Plaintiff's and Class Members' PII because of its value in exploiting and stealing the identities of Plaintiff and

[2] https://ago.vermont.gov/blog/2022/10/31/ethos-group-data-breach-notice-to-consumers/?utm_source=rss&utm_medium=rss&utm_campaign=ethos-group-data-breach-notice-to-consumers
[3] *Id.*
[4] https://apps.web.maine.gov/online/aeviewer/ME/40/c1af9d00-86a4-4dab-ae18-faeff7ec9058.shtml

Class Members. The present and continuing risk to victims of the Data Breach will remain for their respective lifetimes.

9. Plaintiff brings this action on behalf of all persons whose PII was compromised as a result of Defendant's failure to: (i) adequately protect the PII of Plaintiff and Class Members; (ii) warn Plaintiff and Class Members of Defendant's inadequate information security practices; and (iii) effectively secure hardware containing protected PII using reasonable and effective security procedures free of vulnerabilities and incidents. Defendant's conduct amounts to negligence, at the minimum, and violates federal and state statutes.

10. Plaintiff and Class Members have suffered injury as a result of Defendant's conduct. These injuries include: (i) lost or diminished value of PII ; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time, and (iv) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) may remain backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII .

11. Defendant disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, or negligently failing to implement and maintain adequate and reasonable measures to ensure that the PII of Plaintiff and Class Members was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required, and appropriate protocols, policies, and procedures regarding the encryption of data, even for internal use. As a result, the PII of Plaintiff and Class Members was compromised

through disclosure to an unknown and unauthorized third party. Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

II. PARTIES

12. Plaintiff Nicholas Gorman is and has been at all relevant times a resident and citizen of Illinois, currently residing in Girard, Illinois. Mr. Gorman received the Notice Letter, via U.S. mail, directly from Defendant, dated November 2, 2022.

13. If Mr. Gorman had known that Defendant would not adequately protect his PII, he would not have entrusted his PII to Defendant or allowed Defendant to maintain this sensitive and PII.

14. Defendant Ethos Group, Inc. is a business incorporated under the state laws of Texas, with its principal place of business located at 3070 Las Colinas Blvd. West, Suite 108, Irving, Texas, 75039, in the Dallas Division of the Northern District of Texas.

15. The true names and capacities of persons or entities, whether individual, corporate, associate, or otherwise, who may be responsible for some of the claims alleged herein are currently unknown to Plaintiff. Plaintiff will seek leave of court to amend this complaint to reflect the true names and capacities of such other responsible parties when their identities become known.

16. All of Plaintiff's claims stated herein are asserted against Defendant and any of its owners, predecessors, successors, subsidiaries, agents and/or assigns.

III. JURISDICTION AND VENUE

17. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. § 1332(d). The amount in controversy exceeds the sum of

$5,000,000 exclusive of interest and costs, there are more than 100 putative class members, and minimal diversity exists because many putative class members, including Plaintiff, are citizens of a different state than Defendant. This Court also has supplemental jurisdiction pursuant to 28 U.S.C. § 1367(a) because all claims alleged herein form part of the same case or controversy.

18. This Court has personal jurisdiction over Defendant because it operates and maintains its principal place of business in this District and the computer systems implicated in this Data Breach are likely based in this District. Further, Defendant is authorized to and regularly conducts business in this District and makes decisions regarding corporate governance and management of its businesses in this District, including decisions regarding the security measures to protect its customers' PII. By promoting, selling and marketing its products and services from Texas to thousands of consumers nationwide, Defendant intentionally avails itself of this jurisdiction.

19. Venue is proper in this District under 28 U.S.C. § 1391(a) through (d) because a substantial part of the events giving rise to this action occurred in this District, including decisions made by Defendant's governance and management personnel or inaction by those individuals that led to the Data Breach; Defendant's principal place of business is located in this district; Defendant maintains Class Members' PII in this District; and Defendant caused harm to Class Members residing in this District.

IV. FACTUAL ALLEGATIONS

Background

20. Defendant is a Texas-based company that provides a variety of services to its partnered automobile dealership including consulting, recruiting, training, compliance solutions, as well as "financing and servicing automobiles".[5]

21. Plaintiff and Class Members are current and former customers at one or more of Defendant's partner dealerships, and Plaintiff and Class Members obtained an automobile-related service and/or products from Defendant, either directly or indirectly through the partner dealership(s).

22. In order to obtain Defendant's services, Plaintiff and Class Members were required to provide sensitive and confidential PII, including their names, driver's license numbers, and other sensitive and confidential information.

23. Plaintiff and Class Members value the confidentiality of their PII and expected that Defendant, or anyone in Defendant's position, would implement adequate security practices to safeguard the PII it collected from them, that the privacy of that information would be maintained, and that Defendant would delete any sensitive information after it was no longer required to maintain it.

24. Defendant understood that Plaintiff and Class Members expected Defendant to implement reasonable data security practices to safeguard their PII. Indeed, Defendant's Privacy Policy provides that Ethos "is committing to protecting [customers'] privacy".[6] Further, the Privacy Policy specifically states that Ethos "secures the personally identifiable information you

[5] https://www.ethosgroup.com/
[6] http://ethosgroup.com/privacy-policy/#:~:text=Ethos%20Group%20will%20not%20collect,purposes%20without%20providing%20you%20notice..

provide on computer servers in a controlled, secure environment, protected from unauthorized access, use or disclosure."[7]

25. Plaintiff and Class Members relied on the sophistication of Defendant to keep their PII confidential and securely maintained, to use this information for necessary purposes only, and to make only authorized disclosures of this information. Plaintiff and Class Members reasonably expect security to safeguard their PII and would not provide it as part of a transaction absent an implicit promise to protect it.

26. By accepting and using the PII of Plaintiff and Class Members, Defendant assumed a duty to adopt reasonable measures to protect the PII of Plaintiff and Class Members from involuntary disclosure to third parties.

27. Defendant had obligations created by FTC Act, contract, industry standards, and representations made to Plaintiff and Class Members, to keep their PII confidential and to protect it from unauthorized access and disclosure.

28. Plaintiff and Class Members provided their PII to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

The Data Breach

29. On or about November 2, 2022, Defendant began sending Plaintiff and other victims of the Data Breach a Notice of Security Incident letter, informing them that:

> On August 1, 2022, we determined some consumer information was accessed between July 30, 2022 and July 31, 2022. We immediately launched an investigation, with the assistance of third-party cybersecurity specialists, to confirm the nature and scope of the activity. This investigation was completed on October 24, 2022 and confirmed that some of your information was present.

[7] *Id.*

30. Omitted from the Notice Letter were the details of the root cause of the Data Breach, the vulnerabilities exploited, whether Defendant's system is still unsecured, why it took over three months to inform impacted individuals after Defendant first detected the Data Breach, and the remedial measures undertaken to ensure such a breach does not occur again. To date, these omitted details have not been explained or clarified to Plaintiff and Class Members, who retain a vested interest in ensuring that their PII remains protected.

31. Further, Defendant failed to indicate the method of cyberattack and whether the compromised information was retrieved or if it remains in the hands of cybercriminals.

32. The unencrypted PII of Plaintiff and Class Members may end up for sale to identity thieves on the Dark Web, if it has not already, or it could simply fall into the hands of companies that will use the detailed PII for targeted marketing without the approval of Plaintiff and Class Members. Unauthorized individuals can easily access the PII of Plaintiff and Class Members.

33. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive information they were maintaining for Plaintiff and Class Members, causing the exposure of PII, such as encrypting the information or deleting it when it is no longer needed.

34. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[8]

35. To prevent and detect cyber-attacks and/or ransomware attacks Defendant could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is

[8] *See* How to Protect Your Networks from RANSOMWARE, at 3, available at https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (last visited Aug. 23, 2021).

delivered.

- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.

- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.

- Configure firewalls to block access to known malicious IP addresses.

- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.

- Set anti-virus and anti-malware programs to conduct regular scans automatically.

- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.

- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.

- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.

- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.

- Consider disabling Remote Desktop protocol (RDP) if it is not being used.

- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.

- Execute operating system environments or specific programs in a virtualized environment.

- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[9]

[9] *Id.* at 3-4.

36. To prevent and detect cyber-attacks Defendant could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

- **Update and patch your computer.** Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks….

- **Use caution with links and when entering website addresses**. Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net)….

- **Open email attachments with caution**. Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.

- **Keep your personal information safe**. Check a website's security to ensure the information you submit is encrypted before you provide it….

- **Verify email senders**. If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.

- **Inform yourself**. Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.

- **Use and maintain preventative software programs**. Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic….[10]

[10] *See* Security Tip (ST19-001) Protecting Against Ransomware (original release date Apr. 11, 2019), *available at:* https://us-cert.cisa.gov/ncas/tips/ST19-001 (last visited Oct. 17, 2022).

37. To prevent and detect cyber-attacks or ransomware attacks Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Secure internet-facing assets

- Apply latest security updates
- Use threat and vulnerability management
- Perform regular audit; remove privileged credentials;

Thoroughly investigate and remediate alerts

- Prioritize and treat commodity malware infections as potential full compromise;

Include IT Pros in security discussions

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

Build credential hygiene

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords;

Apply principle of least-privilege

- Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events;

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[11]

[11] *See* Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), *available at:* https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/ (last visited Nov. 11, 2021).

38. Given that Defendant was storing the PII entrusted to it by its current and former customers, Defendant could and should have implemented all of the above measures to prevent and detect cyberattacks.

39. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach and the exposure of the PII of over 800,000 individuals,[12] including that of Plaintiff and Class Members.

Defendant Acquires, Collects, and Stores the PII of Plaintiff and Class Members

40. Defendant has historically acquired, collected, and stored the PII of Plaintiff and Class Members.

41. As a condition receiving Defendant's services, whether directly or indirectly through one of Defendant's partner dealerships, Plaintiff and Class Members were required to give their sensitive and confidential PII to Defendant. Defendant retains this information.

42. By obtaining, collecting, and storing the PII of Plaintiff and Class Members, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting the PII from disclosure.

43. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII and relied on Defendant to keep their PII confidential and maintained securely, to use this information for business purposes only, and to make only authorized disclosures of this information.

44. Defendant could have prevented this Data Breach by properly securing and encrypting the files and file servers containing the PII of Plaintiff and Class Members.

[12] https://apps.web.maine.gov/online/aeviewer/ME/40/c1af9d00-86a4-4dab-ae18-faeff7ec9058.shtml

45. Defendant's Privacy Policy and other conduct and representations demonstrate its understanding of the importance of securing PII.

46. Defendant's negligence in safeguarding the PII of Plaintiff and Class Members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

47. In light of recent high profile data breaches at other industry leading companies, including, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Defendant knew or should have known that its electronic records would be targeted by cybercriminals.

48. Indeed, cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued warnings to potential targets so they are aware of, and prepared for, a potential attack.

49. Defendant failed to take appropriate steps to protect the PII of Plaintiff and Class Members from being compromised.

50. Defendant Knew or Should Have Known of the Risk because Financing Companies in Possession of PII are Particularly Susceptible to Cyber Attacks due to the volume of sensitive information that they maintain.

51. Defendant's data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches targeting entities that collect and store PII, like Defendant, preceding the date of the breach.

52. Data breaches, including those perpetrated against financing companies that store PII or other sensitive information in in their systems, have become widespread.

53. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.[13]

54. The 330 reported breaches reported in 2021 exposed nearly 30 million sensitive records (28,045,658), compared to only 306 breaches that exposed nearly 10 million sensitive records (9,700,238) in 2020.[14]

55. Indeed, cyber-attacks, such as the one experienced by Defendant, have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. As one report explained, smaller entities that store PII are "attractive to ransomware criminals…because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[15]

56. Defendant knew and understood that unprotected or exposed PII in the custody of financing companies, like Defendant, is valuable and highly sought after by nefarious third parties seeking to illegally monetize that PII through unauthorized access.

57. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiff and Class Members and of the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

---

[13] *See* 2021 Data Breach Annual Report (ITRC, Jan. 2022) (available at https://notified.idtheftcenter.org/s/), at 6.

[14] ***Id.***

[15] https://www.law360.com/consumerprotection/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware?nl_pk=3ed44a08-fcc2-4b6c-89f0-aa0155a8bb51&utm_source=newsletter&utm_medium=email&utm_campaign=consumerprotection (last accessed Oct. 17, 2022).

58. Defendant's knowledge of the foreseeable risk of a cyber-attack, like the one Defendant experienced, is demonstrated, in part, by its Privacy Policy.[16]

59. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII .

60. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's server(s), amounting to potentially over 800,000 individuals' detailed PII,[17] and, thus, the significant number of individuals who would be harmed by the exposure of their unencrypted data.

61. Defendant's knowledge of the present and continuing risk to Plaintiff and Class Members is evidenced by its Notice Letter which warns recipients to "remain vigilant" by monitoring their credit reports for evidence of fraud or identity theft. Despite this, Defendant has done nothing to help the impacted persons prevent or mitigate the misuse of their PII, and has not even offered to provide identity monitoring services for any duration of time. This leaves Plaintiff and Class Members to pay out of pocket for services necessary to mitigate or prevent the harms resulting from the Data Breach.

62. Plaintiff and Class Members have not been compensated for the injuries arising from the Data Breach. Victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft, financial fraud, which they are forced to pay for on their own despite having no culpability in the Data Breach making the monitoring necessary.

---

[16] Defendant's Privacy Policy provides that Defendant may deny customers' requests to delete their data if retaining the information is necessary for "detect[ing] security incidents, protect against malicious, deceptive, fraudulent, or illegal activity[.]" *See* http://ethosgroup.com/privacy-policy/#:~:text=Ethos%20Group%20will%20not%20collect,purposes%20without%20providing%20you%20notice.

[17] https://apps.web.maine.gov/online/aeviewer/ME/40/c1af9d00-86a4-4dab-ae18-faeff7ec9058.shtml

63. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII of Plaintiff and Class Members.

64. The ramifications of Defendant's failure to keep secure the PII of Plaintiff and Class Members are long lasting and severe. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.

65. As a financing company in custody of former and current customers' PII, Defendant knew, or should have known, the importance of safeguarding PII entrusted to them by Plaintiff and Class Members, and of the foreseeable consequences if its data security systems were breached. This includes the significant costs imposed on Plaintiff and Class Members as a result of a breach. Nonetheless, Defendant failed to take adequate cybersecurity measures to prevent the Data Breach.

Value of Personally Identifiable Information

66. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[18] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[19]

67. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity

[18] 17 C.F.R. § 248.201 (2013).
[19] *Id.*

credentials.[20] For example, Personal Information can be sold at a price ranging from $40 to $200.[21] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[22]

68. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information . . . are worth more than 10x on the black market."[23]

69. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

70. Identity thieves also frequently use driver's licenses, the driver's license photo identification, and driver license's numbers as methods of "confirming" their false identity so as to open fraudulent accounts under a victim's name or conduct other fraudulent activity.

71. Identity thieves use personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[24] According to Experian, one of the largest credit reporting companies in the world, "[t]he research shows that personal information is valuable to identity thieves, and if they can get access to it, they will use it" to among other things: open a new credit card or loan, change a billing address so the victim no longer receives bills, open

[20] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last visited Oct. 17, 2022).
[21] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited Oct. 17, 2022).
[22] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last visited Oct. 217, 2022).
[23] Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), *available at*: https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited Oct. 17, 2022).
[24] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 12 C.F.R. § 1022.3(h). The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." 12 C.F.R. § 1022.3(g).

new utilities, obtain a mobile phone, open a bank account and write bad checks, use a debit card number to withdraw funds, obtain a new driver's license or ID, and/or use the victim's information in the event of arrest or court action.[25]

72. Because a person's identity is akin to a puzzle with multiple data points, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity or track the victim to attempt other hacking crimes against the individual to obtain more data to perfect a crime.

73. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate and trick individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails. Data Breaches can be the starting point for these additional targeted attacks on the victims.

74. Each year, identity theft causes tens of billions of dollars of losses to victims in the United States.[26] For example, the driver's license and state issued identification information stolen in the Data Breach can be used to create fake driver's licenses, open accounts in your name, avoid traffic tickets or collect government benefits such as unemployment checks.[27] These criminal activities have and will result in devastating financial and personal losses to Plaintiff and Class Members.

---

[25] Susan Henson, *What Can Identity Thieves Do with Your Personal Information and How Can You Protect Yourself?*, EXPERIAN (Sept. 1, 2017), https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/ (last visited December 13, 2022).

[26] "Facts + Statistics: Identity Theft and Cybercrime," Insurance Info. Inst., https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (discussing Javelin Strategy & Research's report "2018 Identity Fraud: Fraud Enters a New Era of Complexity").

[27] https://www.experian.com/blogs/ask-experian/what-should-i-do-if-my-drivers-license-number-is-stolen/.

75. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change as it represents static information, i.e. including names and driver licenses.

76. The fraudulent activity resulting from the Data Breach may not come to light for years. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[28]

Defendant Fails to Comply with FTC Guidelines

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

78. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. These guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer

[28] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* https://www.gao.gov/assets/gao-07-737.pdf (last visited Oct. 17, 2022).

networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[29]

79. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[30]

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

81. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

82. These FTC enforcement actions include actions against financing companies, like Defendant. *See, e.g., In re Cap. One Consumer Data Sec. Breach Litig.*, 488 F. Supp. 3d 374, 408 (E.D. Va. 2020) *("*"Plaintiffs have plausibly alleged a claim" based upon violation of Section 5 of the FTC Act.)

[29] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016). Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Oct. 17, 2022).
[30] *Id.*

83. Defendant failed to properly implement basic data security practices.

84. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to current and former customers' PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

85. Upon information and belief, Defendant was at all times fully aware of its obligation to protect the PII of its customers. Defendant was also aware of the significant repercussions that would result from its failure to do so.

Defendant Violated the Gramm-Leach-Bliley Act

86. Defendant is a financial institution, as that term is defined by Section 509(3)(A) of the Gramm-Leach-Bliley Act ("GLBA"), 15 U.S.C. § 6809(3)(A), and thus is subject to the GLBA.

87. The GLBA defines a financial institution as "any institution the business of which is engaging in financial activities as described in Section 1843(k) of Title 12 [The Bank Holding Company Act of 1956]." 15 U.S.C. § 6809(3)(A).

88. Defendant collects nonpublic personal information, as defined by 15 U.S.C. § 6809(4)(A), 16 C.F.R. § 313.3(n) and 12 C.F.R. § 1016.3(p)(1). Accordingly, during the relevant time period, Defendant was subject to the requirements of the GLBA, 15 U.S.C. §§ 6801.1, *et seq*., and is subject to numerous rules and regulations promulgated on the GLBA statutes.

89. The GLBA Privacy Rule became effective on July 1, 2001. *See* 16 C.F.R. Part 313. Since the enactment of the Dodd-Frank Act on July 21, 2010, the CFPB became responsible for implementing the Privacy Rule. In December 2011, the CFPB restated the implementing regulations in an interim final rule that established the Privacy of Consumer Financial

Information, Regulation P, 12 C.F.R. § 1016 ("Regulation P"), with the final version becoming effective on October 28, 2014.

90. Accordingly, Defendant's conduct is governed by the Privacy Rule prior to December 30, 2011 and by Regulation P after that date.

91. Both the Privacy Rule and Regulation P require financial institutions to provide customers with an initial and annual privacy notice. These privacy notices must be "clear and conspicuous." 16 C.F.R. §§ 313.4 and 313.5; 12 C.F.R. §§ 1016.4 and 1016.5. "Clear and conspicuous means that a notice is reasonably understandable and designed to call attention to the nature and significance of the information in the notice." 16 C.F.R. § 313.3(b)(1); 12 C.F.R. § 1016.3(b)(1). These privacy notices must "accurately reflect[] [the financial institution's] privacy policies and practices." 16 C.F.R. § 313.4 and 313.5; 12 C.F.R. §§ 1016.4 and 1016.5. They must include specified elements, including the categories of nonpublic personal information the financial institution collects and discloses, the categories of third parties to whom the financial institution discloses the information, and the financial institution's security and confidentiality policies and practices for nonpublic personal information. 16 C.F.R. § 313.6; 12 C.F.R. § 1016.6. These privacy notices must be provided "so that each consumer can reasonably be expected to receive actual notice." 16 C.F.R. § 313.9; 12 C.F.R. § 1016.9. As alleged herein, Defendant violated the Privacy Rule and Regulation P.

92. Defendant failed to provide annual privacy notices to customers after the customer relationship ended, despite retaining these customers' PII and storing that PII on Defendant's network systems.

93. Defendant failed to adequately inform its customers that it was storing and/or sharing, or would store and/or share, the customers' PII on an insecure platform, accessible to unauthorized parties from the internet, and would do so after the customer relationship ended.

94. The Safeguards Rule, which implements Section 501(b) of the GLBA, 15 U.S.C. § 6801(b), requires financial institutions to protect the security, confidentiality, and integrity of customer information by developing a comprehensive written information security program that contains reasonable administrative, technical, and physical safeguards, including: (1) designating one or more employees to coordinate the information security program; (2) identifying reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information, and assessing the sufficiency of any safeguards in place to control those risks; (3) designing and implementing information safeguards to control the risks identified through risk assessment, and regularly testing or otherwise monitoring the effectiveness of the safeguards' key controls, systems, and procedures; (4) overseeing service providers and requiring them by contract to protect the security and confidentiality of customer information; and (5) evaluating and adjusting the information security program in light of the results of testing and monitoring, changes to the business operation, and other relevant circumstances. 16 C.F.R. §§ 314.3 and 314.4. As alleged herein, Defendant violated the Safeguard Rule.

95. Defendant failed to assess reasonably foreseeable risks to the security, confidentiality, and integrity of customer information.

96. Defendant violated the GLBA and its own policies and procedures by sharing the PII of Plaintiff and Class Members with a non-affiliated third party without providing Plaintiff and Class Members (a) an opt-out notice and (b) a reasonable opportunity to opt out of such disclosure.

Defendant Fails to Comply with Industry Standards

97. As noted above, experts studying cyber security routinely identify entities in possession of PII as being particularly vulnerable to cyberattacks because of the value of the PII which they collect and maintain.

98. Several best practices have been identified that, at a minimum, should be implemented by financing companies in possession of PII, like Defendant, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data and limiting which employees can access sensitive data. Defendant failed to follow these industry best practices, including a failure to implement multi-factor authentication.

99. Other best cybersecurity practices that are standard in the financing 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; training staff regarding critical points. Defendant failed to follow these cybersecurity best practices, including failure to train staff.

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

101. These foregoing frameworks are existing and applicable industry standards in the financing industry, and upon information and belief, Defendant failed to comply with at least one––or all—of these accepted standards, thereby opening the door to the threat actor and causing the Data Breach.

COMMON INJURIES & DAMAGES

102. As a result of Defendant's ineffective and inadequate data security practices, the Data Breach, and the foreseeable consequences of PII ending up in the possession of criminals, the risk of identity theft to the Plaintiff and Class Members has materialized and is imminent, and Plaintiff and Class Members have all sustained actual injuries and damages, including: (a) invasion of privacy; (b) "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (c) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (d) the loss of benefit of the bargain (price premium damages); (e) diminution of value of their Private Information; and (f) the continued risk to their PII, which remains in the possession of Defendant, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' PII .

The Data Breach Increases Plaintiff's and Class Member's Risk of Identity Theft

103. The unencrypted PII of Plaintiff and Class Members will end up for sale on the dark web as that is the *modus operandi* of hackers.

104. Unencrypted PII may also fall into the hands of companies that will use the detailed PII for targeted marketing without the approval of Plaintiff and Class Members. Simply, unauthorized individuals can easily access the PII of Plaintiff and Class Members.

105. The link between a data breach and the risk of identity theft is direct and well established. Criminals acquire and steal PII to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

106. Plaintiff's and Class Members' PII is of great value to hackers and cyber criminals, and the data stolen in the Data Breach has been used and will continue to be used in a variety of sordid ways for criminals to exploit Plaintiff and Class Members and to profit off their misfortune.

Loss of Time to Mitigate the Risk of Identity Theft and Fraud

107. As a result of the recognized risk of identity theft, when a Data Breach occurs, and an individual is notified by a company that their PII was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft of fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm – yet, the resource and asset of time has been lost.

108. Thus, due to the actual and imminent risk of identity theft, Plaintiff and Class Members must, as Defendant's Notice Letter instructs them, "remain vigilant" and monitor their financial accounts for many years to mitigate the risk of identity theft.

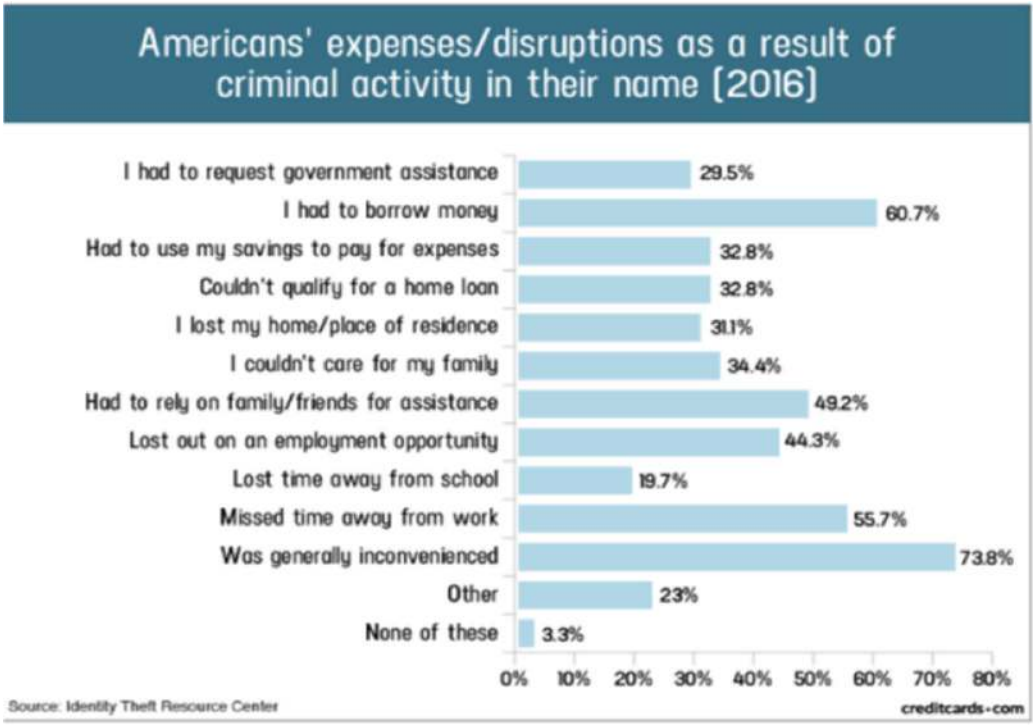
109. Plaintiff and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions, such as placing "freezes" and "alerts" with credit reporting agencies, contacting financial institutions, changing passwords, and reviewing and monitoring credit reports and accounts for unauthorized activity, which may take years to discover and detect.

110. Plaintiff's mitigation efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches ("GAO Report") in

which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[31]

111. Plaintiff's mitigation efforts are also consistent with the steps that FTC recommends that data breach victims take several steps to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[32]

112. A study by Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:[33]



[31] *See* United States Government Accountability Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (June 2007), https://www.gao.gov/new.items/d07737.pdf.
[32] *See* Federal Trade Commission, *Identity Theft.gov*, https://www.identitytheft.gov/Steps (last visited July 7, 2022).
[33] Credit Card and ID Theft Statistics" by Jason Steele, 10/24/2017, at: https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php (last visited Sep 13, 2022).

113. And for those Class Members who experience actual identity theft and fraud, the United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[34]

Diminution of Value of PII

114. PII is a valuable property right.[35] Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that PII has considerable market value.

115. Sensitive PII can sell for as much as $363 per record according to the Infosec Institute.[36]

116. An active and robust legitimate marketplace for PII also exists. In 2019, the data brokering industry was worth roughly $200 billion.[37] In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[38,39]

---

[34] *See* "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," p. 2, U.S. Government Accountability Office, June 2007, https://www.gao.gov/new.items/d07737.pdf (last visited Sep. 13, 2022) ("GAO Report").

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

[36] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/ (last visited Sep. 13, 2022).

[37] https://www.latimes.com/business/story/2019-11-05/column-data-brokers

[38] https://datacoup.com/

[39] https://digi.me/what-is-digime/

Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.[40]

117. As a result of the Data Breach, Plaintiff's and Class Members' PII, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its compromise and unauthorized release. However, this transfer of value occurred without any consideration paid to Plaintiff or Class Members for their property, resulting in an economic loss. Moreover, the PII is now readily available, and the rarity of the Data has been lost, thereby causing additional loss of value.

118. Driver's license numbers are incredibly valuable. "Hackers harvest license numbers because they're a very valuable piece of information. A driver's license can be a critical part of a fraudulent, synthetic identity – which go for about $1200 on the Dark Web. On its own, a forged license can sell for around $200."[41]

119. According to national credit bureau Experian:

> A driver's license is an identity thief's paradise. With that one card, someone knows your birthdate, address, and even your height, eye color, and signature. If someone gets your driver's license number, it is also concerning because it's connected to your vehicle registration and insurance policies, as well as records on file with the Department of Motor Vehicles, place of employment (that keep a copy of your driver's license on file), doctor's office, government agencies, and other entities. Having access to that one number can provide an identity thief with several pieces of information they want to know about you. Next to your Social Security number, your driver's license number is one of the most important pieces of information to keep safe from thieves.[42]

120. According to cybersecurity specialty publication CPO Magazine, "[t]o those unfamiliar with the world of fraud, driver's license numbers might seem like a relatively harmless

---

[40] Nielsen Computer & Mobile Panel, Frequently Asked Questions, available at https://computermobilepanel.nielsen.com/ui/US/en/faqen.html

[41] https://www.forbes.com/sites/leemathews/2021/04/20/hackers-stole-customers-license-numbers-from-geico-in-months-long-breach/?sh=3e4755c38658 (last accessed July 20, 2021)

[42] Sue Poremba, *What Should I Do If My Driver's License Number is Stolen?"* (October 24, 2018) (last accessed July 20, 2021)

piece of information to lose if it happens in isolation."[43] However, this is not the case. As cybersecurity experts point out:

> "It's a gold mine for hackers. With a driver's license number, bad actors can manufacture fake IDs, slotting in the number for any form that requires ID verification, or use the information to craft curated social engineering phishing attacks."[44]

121. Victims of driver's license number theft also often suffer unemployment benefit fraud, as described in a recent New York Times article.[45]

122. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiff and Class Members, and of the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

123. The fraudulent activity resulting from the Data Breach may not come to light for years.

124. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII .

125. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's network, amounting to potentially hundreds of thousands of individuals' detailed personal information and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

---

[43] https://www.cpomagazine.com/cyber-security/geico-data-breach-leaks-drivers-license-numbers-advises-customers-to-watch-out-for-fraudulent-unemployment-claims/ (last accessed July 20, 2021)
[44] *Id.*
[45] *How Identity Thieves Took My Wife for a Ride,* NY Times, April 27, 2021 https://www.nytimes.com/2021/04/27/your-money/identity-theft-auto-insurance.html (last accessed July 20, 2021)

126. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII of Plaintiff and Class Members.

Future Cost of Credit and Identity Theft Monitoring is Reasonable and Necessary

127. Given the type of targeted attack in this case and sophisticated criminal activity, the type of PII, reports of misuse of Class Member PII discussed below, and reports of dissemination on the Dark Web also discussed below, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and purchase by criminals intending to utilize the PII for identity theft crimes –*e.g.*, opening bank accounts in the victims' names to make purchases or to launder money; file false tax returns; take out loans or lines of credit; or file false unemployment claims.

128. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that his or her PII was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

129. Consequently, Plaintiff and Class Members are at an increased risk of fraud and identity theft for many years into the future.

130. In its Notice Letter, Defendant did not offer credit and identity theft monitoring *for any duration of time* to victims of the Data Breach, despite their critical need for the service.

131. The retail cost of credit monitoring and identity theft monitoring can cost around $200 a year per Class Member. This is reasonable and necessary cost to monitor to protect Class Members from the risk of identity theft that arose from Defendant's Data Breach. This is a future

cost for a minimum of five years that Plaintiff and Class Members would not need to bear but for Defendant's failure to safeguard their PII .

Loss of Benefit of the Bargain

132. Furthermore, Defendant's poor data security deprived Plaintiff and Class Members of the benefit of their bargain. When agreeing to pay Defendant, whether directly or indirectly, through one of its partner dealerships for Defendant's products and/or services, Plaintiff and other reasonable consumers understood and expected that they were, in part, paying for the service and necessary data security to protect the PII, when in fact, Defendant did not provide the expected data security. Accordingly, Plaintiff and Class Members received services that were of a lesser value than what they reasonably expected to receive under the bargains they struck with Defendant.

Plaintiff Gorman's Experience

133. Plaintiff Gorman purchased a car from one of Defendant's partner dealerships in or about February 2021. When Mr. Gorman did so, he obtained financing for the vehicle through Defendant. In order to obtain financing services from Defendant, he was required to provide his PII to Defendant.

134. At the time of the Data Breach—from July 30, 2022, through July 31, 2022—Defendant retained Plaintiff's PII in its system.

135. Plaintiff Gorman is very careful about sharing his sensitive PII. Plaintiff stores any documents containing his PII in a safe and secure location. He has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

136. Plaintiff Gorman received the Notice Letter, by U.S. mail, directly from Defendant, dated November 2, 2022. According to the Notice Letter, Plaintiff's PII was improperly accessed and obtained by unauthorized third parties, including his name and driver's license number.

137. As a result of the Data Breach, and at the direction of Defendant's Notice Letter, Plaintiff made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to: researching the Data Breach; reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud; changing passwords and resecuring his own computer system; and researching the credit monitoring and identity theft protection services offered by Defendant. Plaintiff has spent significant time dealing with the Data Breach, valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

138. Plaintiff suffered actual injury from having his PII compromised as a result of the Data Breach including, but not limited to: (a) invasion of privacy; (b) "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (c) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (d) the loss of benefit of the bargain (price premium damages); (e) diminution of value of his Private Information; and (f) present, imminent and impending injury arising from the increased risk of identity theft and fraud.

139. The Data Breach has caused Plaintiff to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed him of key details about the Data Breach's occurrence.

140. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a

result of the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

141. Plaintiff Gorman has a continuing interest in ensuring that his PII, which, upon information and belief, remain backed up in Defendant's possession, is protected and safeguarded from future breaches.

V. CLASS ALLEGATIONS

142. Plaintiff brings this nationwide class action on behalf of himself and on behalf of all others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

143. The Class that Plaintiff seeks to represent is defined as follows:

> All individuals residing in the United States whose PII was accessed and/or acquired by an unauthorized party as a result of the data breach reported by Defendant on or about November 2, 2022 (the "Class").

144. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant have a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

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

146. Numerosity: The members of the Class are so numerous that joinder of all members is impracticable, if not completely impossible. At least 800,000 individuals were notified by Defendant of the Data Breach, according to the breach report submitted to Maine Attorney

General's Office.[46] The Class is apparently identifiable within Defendant's records, and Defendant has already identified these individuals (as evidenced by sending them breach notification letters).

147. Common questions of law and fact exist as to all members of the Class and predominate over any questions affecting solely individual members of the Class. Among the questions of law and fact common to the Class that predominate over questions which may affect individual Class members, including the following:

a. Whether and to what extent Defendant had a duty to protect the PII of Plaintiff and Class Members;

b. Whether Defendant had respective duties not to disclose the PII of Plaintiff and Class Members to unauthorized third parties;

c. Whether Defendant had respective duties not to use the PII of Plaintiff and Class Members for non-business purposes;

d. Whether Defendant failed to adequately safeguard the PII of Plaintiff and Class Members;

e. Whether and when Defendant actually learned of the Data Breach;

f. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their PII had been compromised;

g. Whether Defendant violated the law by failing to promptly notify Plaintiff and Class Members that their PII had been compromised;

h. 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;

[46] https://apps.web.maine.gov/online/aeviewer/ME/40/c1af9d00-86a4-4dab-ae18-faeff7ec9058.shtml

i. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

j. Whether Plaintiff and Class Members are entitled to actual damages, statutory damages, and/or nominal damages as a result of Defendant's wrongful conduct;

k. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

148. Typicality: Plaintiff's claims are typical of those of the other members of the Class because Plaintiff, like every other Class Member, was exposed to virtually identical conduct and now suffers from the same violations of the law as each other member of the Class.

149. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendant acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiff's challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

150. Adequacy: Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that he has no disabling conflicts of interest that would be antagonistic to those of the other Class Members. Plaintiff seeks no relief that is antagonistic or adverse to the Class Members and the infringement of the rights and the damages he has suffered are typical of other Class Members. Plaintiff has retained counsel experienced in complex class action and data breach litigation, and Plaintiff intends to prosecute this action vigorously.

151. Superiority and Manageability: The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

152. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff was exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

153. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class

Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

154. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

155. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the PII of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendant may continue to act unlawfully as set forth in this Complaint.

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

157. Likewise, particular issues under Rule 42(d)(1) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant failed to timely notify the Plaintiff and the class of the Data Breach;

b. Whether Defendant owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their Private Information;

c. Whether Defendant's security measures to protect their data systems were reasonable in light of best practices recommended by data security experts;

d. Whether Defendant's failure to institute adequate protective security measures amounted to negligence;

e. Whether Defendant failed to take commercially reasonable steps to safeguard consumer Private Information; and Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

VI. CAUSES OF ACTION

FIRST CAUSE OF ACTION
Negligence
(On Behalf of Plaintiff and the Class)

158. Plaintiff re-alleges and incorporates by reference the allegations above as if fully set forth herein.

159. Defendant required Plaintiff and Class Members to submit non-public personal information in order to obtain Defendant's financing, other services and/or products.

160. By collecting and storing this data in Defendant's computer property, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and safeguard their computer property—and Class Members' Private Information held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which it could detect a breach of their security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a Data Breach.

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

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

163. Defendant's duty to use reasonable security measures also arose under the GLBA, under which Defendant was required to protect the security, confidentiality, and integrity of customer information by developing a comprehensive written information security program that contains reasonable administrative, technical, and physical safeguards.

164. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and its customers. That special relationship arose because Plaintiff and the Class entrusted Defendant with their confidential PII, a necessary part of being customers of Defendant.

165. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential Private Information.

166. Defendant was subject to an "independent duty," untethered to any contract between Defendant and Plaintiff or the Class.

167. Defendant also had a duty to exercise appropriate clearinghouse practices to remove former customers' PII it was no longer required to retain pursuant to regulations.

168. Defendant also had a duty to have procedures in place to detect and prevent the improper access and misuse of the PII of Plaintiff and the Class.

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

- Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;
- Failing to adequately monitor the security of their networks and systems;
- Failure to periodically ensure that their email system had plans in place to maintain reasonable data security safeguards;
- Allowing unauthorized access to Class Members' Private Information;
- Failing to detect in a timely manner that Class Members' Private Information had been compromised;
- Failing to remove former customers' PII it was no longer required to retain pursuant to regulations,
- Failing to timely and adequately notify Class Members about the Data Breach's occurrence and scope, so that they could take appropriate steps to mitigate the potential for identity theft and other damages; and
- Failing to secure its stand-alone personal computers, such as the reception desk computers, even after discovery of the data breach.

170. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Class was reasonably foreseeable, particularly in light of Defendant's inadequate security practices.

171. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' Private Information would result in injury to Class Members. Further, the breach

of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in both the financial services and medical industry.

172. Defendant has full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and the Class could and would suffer if the PII were wrongfully disclosed.

173. Plaintiff and the Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the PII of Plaintiff and the Class, the critical importance of providing adequate security of that PII, and the necessity for encrypting PII stored on Defendant's systems.

174. It was therefore foreseeable that the failure to adequately safeguard Class Members' Private Information would result in one or more types of injuries to Class Members.

175. Plaintiff and the Class had no ability to protect their PII that was in, and possibly remains in, Defendant's possession.

176. Defendant was in a position to protect against the harm suffered by Plaintiff and the Class as a result of the Data Breach.

177. Defendant had and continues to have a duty to adequately disclose that the PII of Plaintiff and the Class within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiff and the Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII by third parties.

178. Defendant has admitted that the PII of Plaintiff and the Class was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

179. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and the Class, the PII of Plaintiff and the Class would not have been compromised.

180. There is a close causal connection between Defendant's failure to implement security measures to protect the PII of Plaintiff and the Class and the harm, or risk of imminent harm, suffered by Plaintiff and the Class. The PII of Plaintiff and the Class was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

181. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Class.

182. Defendant's violation of Section 5 of the FTC Act constitutes negligence.

183. Defendant violated the GLBA, its Privacy Rule and/or Regulation P, and its Safeguards Rule by (a) failing to provide annual privacy notices to customers after the customer relationship ended, despite retaining these customers' PII and storing and/or sharing that PII on Defendant's internal systems that were inadequately secured and accessible to unauthorized third-parties from the internet, (b) failing to adequately inform its customers that it was storing and/or sharing, or would store and/or share, the customers' PII on such an insecure platform and/or system, (c) failing to assess reasonably foreseeable risks to the security, confidentiality, and integrity of customer information, (d) failed to adequately (i) test and/or monitor the system where the Data Breach occurred and (ii) update and/or further secure its data security practices in light of the heightened risk environment.

184. Defendant's violation of the GLBA, its Privacy Rule and/or Regulation P, and its Safeguards Rule constitutes negligence.

185. Plaintiff and the Class are within the class of persons that the FTC Act and the GLBA were intended to protect.

186. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class. The GLBA, with its Privacy Rule, Regulation P, and Safeguards Rule, was similarly intended to guard against harms such as the harm that occurred as a result of the Data Breach.

187. As a direct and proximate result of Defendant's negligence, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) the loss of the opportunity of how their PII is used; (ii) the compromise, publication, and/or theft of their PII; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (iv) lost opportunity costs associated with effort expended and the loss of productivity 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 tax fraud and identity theft; (v) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII of Plaintiff and the Class; and (vi) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and the Class.

188. As a direct and proximate result of Defendant's negligence, Plaintiff and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not

limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

189. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiff and the Class have suffered and will suffer the continued risks of exposure of their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in its continued possession.

190. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

191. Defendant's negligent conduct is ongoing, in that it still holds the Private Information of Plaintiff and Class Members in an unsafe and unsecure manner.

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

SECOND CAUSE OF ACTION
Breach of Third-Party Beneficiary Contract
(On Behalf of Plaintiff and the Class)

193. Plaintiff re-alleges and incorporates by reference the allegations above as if fully set forth herein.

194. Defendant entered into written contracts, including with its clients to perform services that include, but are not limited to, financing automobile purchases. Upon information and belief, these contracts are virtually identical between and among Defendant and its partnered automobile dealerships around the country whose customers were affected by the Data Breach.

195. In exchange, Defendant agreed, in part, to implement adequate security measures to safeguard the Private Information of Plaintiff and the Class and to timely and adequately notify them of the Data Breach.

196. These contracts were made expressly for the benefit of Plaintiff and the Class, as Plaintiff and Class Members were the intended third-party beneficiaries of the contracts entered into between Defendant and its clients. In entering into these contracts, Defendant and its clients intended to secure a benefit to Plaintiff and Class Members, i.e., the protection of Plaintiff and Class Members Private Information, and entered into the contract directly for the benefit of Class Members and Plaintiff.

197. Defendant knew that if it were to breach these contracts with its clients, the clients' customers—Plaintiff and Class Members—would be harmed.

198. Defendant breached the contracts it entered into with its clients by, among other things, failing to (i) use reasonable data security measures, (ii) implement adequate protocols and employee training sufficient to protect Plaintiff's Private Information from unauthorized disclosure to third parties, and (iii) promptly and adequately notify Plaintiff and Class Members of the Data Breach.

199. Plaintiff and the Class were harmed by Defendant's breach of its contracts with its clients, as such breach is alleged herein, and are entitled to the losses and damages they have sustained as a direct and proximate result thereof.

200. Plaintiff and Class Members are also entitled to their costs and attorney's fees incurred in this action.

THIRD CAUSE OF ACTION
Negligence *Per Se*
(On Behalf of Plaintiff and the Class)

201. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

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

203. Pursuant to the GLBA, Defendant had a duty to protect the security, confidentiality, and integrity of customer information by developing a comprehensive written information security program that contains reasonable administrative, technical, and physical safeguards. 16 C.F.R. §§ 314.3 and 314.4.

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

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

206. Plaintiff and Class Members are within the class of persons the statutes were intended to protect and the harm to Plaintiff and Class Members resulting from the Data Breach was the type of harm against which the statutes were intended to prevent.

207. But for Defendant's wrongful and negligent breach of their duties owed to Plaintiff and Class Members, Plaintiff and Class Members would not have been injured.

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

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

FOURTH CAUSE OF ACTION
Breach of Confidence
(On Behalf of Plaintiff and the Class)

210. Plaintiff re-alleges and incorporates by reference the allegations above as if fully set forth herein.

211. At all times during Plaintiff's and Class members' interactions with Defendant, Defendant was fully aware of the confidential and sensitive nature of Plaintiff's and Class members' PII that Plaintiff and Class members provided to Defendant.

212. As alleged herein and above, Defendant's relationship with Plaintiff and Class members was governed by terms and expectations that Plaintiff's and Class members' PII would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

213. Plaintiff and Class members provided their respective PII to Defendant with the explicit and implicit understandings that Defendant would protect and not permit the information to be disseminated to any unauthorized parties.

214. Plaintiff and Class members also provided their PII to Defendant with the explicit and implicit understandings that Defendant would take precautions to protect that PII from unauthorized disclosure, such as following basic principles of protecting its networks and data systems.

215. Defendant required and voluntarily received, in confidence, Plaintiff's and Class members' PII with the understanding that the information would not be disclosed or disseminated to the public or any unauthorized third parties.

216. Due to Defendant's failure to prevent, detect, and avoid the Data Breach from occurring by, *inter alia*, following best information security practices to secure Plaintiff's and Class members' PII, Plaintiff's and Class members' PII was disclosed to, and misappropriated by, unauthorized third parties beyond Plaintiff's and Class members' confidence, and without their express permission. As a direct and proximate cause of Defendant's actions and/or omissions, Plaintiff and Class members have suffered, and will continue to suffer damages.

217. But for Defendant's disclosure of Plaintiff's and Class members' PII in violation of the parties' understanding of confidence, Plaintiff's and Class Members' PII would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. Defendant's Data Breach was the direct and legal cause of the theft of Plaintiff's and Class members' PII, as well as the resulting damages.

218. The injury and harm Plaintiff and Class members suffered, and continue to suffer, was the reasonably foreseeable result of Defendant's unauthorized disclosure of Plaintiff's and Class members' PII. Defendant knew its computer systems and technologies for accepting and securing Plaintiff's and Class members' PII had numerous security and other vulnerabilities placing Plaintiff's and Class members' PII in jeopardy.

219. As a direct and proximate result of Defendant's breaches of confidence, Plaintiff and Class members have suffered and will suffer injury, including but not limited to: (a) the diminished value of Defendant's services they received; (b) the compromise, publication, and/or theft of their PII; (c) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their PII; (d) lost opportunity costs associated with effort expended and the loss of productivity 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; (e) the continued risk to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in its continued possession; and (f) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiff and Class members.

220. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff and Class members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non–economic losses.

FIFTH CAUSE OF ACTION
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

221. Plaintiff re-alleges and incorporates by reference the allegations above as if fully set forth herein.

222. This count is plead in the alternative to Count II (Breach of Third-Party Beneficiary Contract).

223. Upon information and belief, Defendant funds its data security measures entirely from its general revenue, including payments made by or on behalf of Plaintiff and the Class Members.

224. As such, a portion of the payments made by or on behalf of Plaintiff and the Class Members is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Defendant.

225. Plaintiff and Class Members conferred a monetary benefit on Defendant. Specifically, they made payments to Defendant and/or its agents and in so doing provided Defendant with their Private Information. In exchange, Plaintiff and Class Members should have received from Defendant the services that were the subject of the transaction and have had their Private Information protected with adequate data security.

226. Defendant knew that Plaintiff and Class Members conferred a benefit which Defendant accepted. Defendant profited from these transactions and used the Private Information of Plaintiff and Class Members for business purposes.

227. In particular, Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff's and Class Members' Personal Information. Instead of providing a reasonable level of security that would have prevented the hacking incident, Defendant instead calculated to increase their own profits at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite security.

228. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiff and Class Members, because Defendant

failed to implement appropriate data management and security measures that are mandated by industry standards.

229. Defendant failed to secure Plaintiff's and Class Members' Private Information and, therefore, did not provide full compensation for the benefit Plaintiff and Class Members provided.

230. Defendant acquired the Private Information through inequitable means in that it misrepresented the extent of its data security practices and failed to disclose the inadequate security practices previously alleged.

231. If Plaintiff and Class Members knew that Defendant had not reasonably secured their Private Information, they would not have agreed to provide their Private Information to Defendant.

232. Plaintiff and Class Members have no adequate remedy at law.

233. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

234. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiff and Class Members overpaid for Defendant's services.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and Class Members, requests judgment against Defendant and that the Court grants the following:

A. For an order certifying the Class, as defined herein, and appointing Plaintiff and his Counsel to represent the Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the PII of Plaintiff and Class Members, and from refusing to issue prompt, complete, any accurate disclosures to Plaintiff and Class Members;

C. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state, or local laws;

iii. requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiff and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiff and Class Members;

v. prohibiting Defendant from maintaining the PII of Plaintiff and Class Members on a cloud-based database;

vi. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct

testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

ix. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

x. requiring Defendant to conduct regular database scanning and securing checks;

xi. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;

xii. requiring Defendant to conduct internal training and education routinely and continually, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. requiring Defendant to implement a system of tests to assess its employees' knowledge of the education programs discussed in the preceding

subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

xiv. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential PII to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and for a period of 10 years, appointing a qualified and independent third-party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

D. For an award of damages, including actual, statutory, nominal, and consequential damages, as allowed by law in an amount to be determined;

E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For prejudgment interest on all amounts awarded; and

G. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands that this matter be tried before a jury.

Dated: 12/23/2022

Respectfully submitted,

s/ Joe Kendall

JOE KENDALL
Texas Bar No. 11260700
KENDALL LAW GROUP, PLLC
3811 Turtle Creek Blvd., Suite 1450
Dallas, Texas 75219
214-744-3000 / 214-744-3015 (Facsimile)
jkendall@kendalllawgroup.com

GARY M. KLINGER*
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Phone: (866) 252-0878
gklinger@milberg.com

**pro hac vice forthcoming*

Attorney for Plaintiff and the Class