UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF INDIANA

BRIAN BAKER, on behalf of himself individually and on behalf of all others similarly situated, Plaintiff, v. SLT LENDING SPV, INC. d/b/a SUR LA TABLE, Defendant.	CAUSE NO.: 2:23-CV-190-PPS-JPK
LUANN PETRULAKIS, on behalf of herself individually and on behalf of all others similarly situated, Plaintiff, v. SLT LENDING SPV, INC. d/b/a SUR LA TABLE, Defendant.	
JAMELAH ELDER, on behalf of herself individually and on behalf of all others similarly situated, Plaintiff, v. SLT LENDING SPV, INC. d/b/a SUR LA TABLE, Defendant.	

CONSOLIDATED CLASS ACTION COMPLAINT

Plaintiffs Brian Baker, Luann Petrulakis, and Jamelah Elder ("Plaintiffs"), bring this Class Action Complaint ("Complaint") against Defendant SLT Lending SPV, Inc. d/b/a Sur La Table ("SLT Lending" or "Defendant") as individuals and on behalf of all others similarly situated, and allege, upon personal knowledge as to their own actions and their counsels' investigation, and upon information and belief as to all other matters, as follows:

NATURE OF THE ACTION

1. This class action arises out of the recent cyberattack and data breach ("Data Breach") resulting from SLT Lending failure to implement reasonable and industry standard data security practices.

2. SLT Lending is a nationwide retailer that sells products including food, cookware, bakeware, knives, small appliances, and other kitchen tools.[1]

3. Plaintiffs' and Class Members' sensitive personal information—which they entrusted to Defendant on the mutual understanding that Defendant would protect it against disclosure—was compromised and unlawfully accessed due to the Data Breach.

4. SLT Lending collected and maintained certain personally identifiable information of Plaintiffs and the putative Class Members (defined below), who are (or were) employees at SLT Lending.

5. The Private Information compromised in the Data Breach included Plaintiffs' and Class Members' full names, driver's license numbers or state identification numbers, ("personally identifiable information" or "PII") and medical and health insurance information, which is

[1] https://www.surlatable.com/ (last accessed June 5, 2023)

protected health information ("PHI," and collectively with PII, "Private Information") as defined by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA").

6. The Private Information compromised in the Data Breach was exfiltrated by cyber-criminals and remains in the hands of those cyber-criminals who target Private Information for its value to identity thieves.

7. As a result of the Data Breach, Plaintiffs and potentially thousands of Class Members, suffered concrete injury in fact including, but not limited to: (i) fraudulent charges (as Plaintiffs experienced to his debit card); (ii) lost or diminished value of their Private Information; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; (iv) invasion of privacy; (v) loss of benefit of the bargain; and (vi) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains 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 Private Information.

8. The Data Breach was a direct result of Defendant's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect its employees' Private Information from a foreseeable and preventable cyber-attack.

9. Defendant maintained the Private Information in a reckless manner. In particular, the Private Information was maintained on Defendant's computer network in a condition vulnerable to cyberattacks. Upon information and belief, the mechanism of the cyberattack and potential for improper disclosure of Plaintiffs' and Class Members' Private Information was a

known risk to Defendant, and thus, Defendant was on notice that failing to take steps necessary to secure the Private Information from those risks left that property in a dangerous condition.

10. Defendant disregarded the rights of Plaintiffs and Class Members by, *inter alia*, intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions; failing to disclose that they did not have adequately robust computer systems and security practices to safeguard Class Members' Private Information; failing to take standard and reasonably available steps to prevent the Data Breach; and failing to provide Plaintiffs and Class Members prompt and accurate notice of the Data Breach.

11. Plaintiffs' and Class Members' identities are now at risk because of Defendant's negligent conduct because the Private Information that Defendant collected and maintained is now in the hands of data thieves.

12. Armed with the Private Information accessed in the Data Breach, data thieves have already engaged in identity theft and fraud (including the fraud suffered by Plaintiffs described below), and can in the future commit a variety of crimes including, *e.g.*, opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

13. As a result of the Data Breach, Plaintiffs and Class Members have been exposed to a heightened and imminent risk of fraud and identity theft. Plaintiffs and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft.

14. Plaintiffs and Class Members may also incur out of pocket costs for, *e.g.*, purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

15. Plaintiffs bring this class action lawsuit on behalf of those similarly situated to address Defendant's inadequate safeguarding of Class Members' Private Information that it collected and maintained, and for failing to provide timely and adequate notice to Plaintiffs and other Class Members that their information had been subject to the unauthorized access by an unknown third party and precisely what specific type of information was accessed.

16. Through this Complaint, Plaintiffs seek to remedy these harms on behalf of themselves and all similarly situated individuals whose Private Information was accessed during the Data Breach.

17. Plaintiffs seek remedies including, but not limited to, compensatory damages and injunctive relief including improvements to Defendant's data security systems, future annual audits, and adequate credit monitoring services funded by Defendant.

PARTIES

18. Plaintiff Brian Baker is a resident and citizen of Texas.

19. Plaintiff Luann Petrulakis is a resident and citizen of Illinois.

20. Plaintiff Jamelah Elder is a resident and citizen of California.

21. Defendant SLT Lending is a corporation duly formed and existing under the laws of the State of Delaware with a principal place of business at 8450 Broadway, Merrillville, Indiana 46410.

JURISDICTION AND VENUE

22. 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 each of Plaintiffs, 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.

23. 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 employees' Private Information.

24. 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' Private Information in this District; and Defendant caused harm to Class Members residing in this District.

STATEMENT OF FACTS

Defendant's Business

25. SLT Lending is a retailer that sells products including food, cookware, bakeware, knives, small appliances, and other kitchen tools.[2]

26. Upon information and belief, in the course of collecting Private Information from employees, including Plaintiffs, Defendant promised to provide confidentiality and adequate security for employee data through its applicable privacy policy and through other disclosures in compliance with statutory privacy requirements.

27. Indeed, Defendant's Privacy Policy provides that: "[w]e have implemented measures designed to secure your Personal Information from accidental loss and from unauthorized access, use, alteration, and disclosure. All information you provide to us is stored on our secure servers behind firewalls. Any payment transactions will be encrypted using SSL technology."[3]

28. Even more, the Privacy Policy demonstrates Defendant's awareness of the foreseeability of a cyberattack, like the one it experienced: "[u]nfortunately, the transmission of information via the internet is not completely secure. Although we do our best to protect your Personal Information, we cannot guarantee the security of your Personal Information transmitted to our Website."[4]

29. Plaintiffs and the Class Members, as former and current employees of Defendant, relied on these promises and on this sophisticated business entity to keep their sensitive Private Information confidential and securely maintained, to use this information for business purposes

[2] https://www.surlatable.com/ (last accessed June 5, 2023)
[3] https://www.surlatable.com/privacy-policy.html (last accessed June 5, 2023)
[4] *Id.*

only, and to make only authorized disclosures of this information. Employees, in general, demand security to safeguard their Private Information, especially when their health information, medical information, and other sensitive Private Information is involved.

30. In the course of their employment relationship, employees, including Plaintiffs and Class Members, provided Defendant with at least the following Private Information:

a. names;

b. driver's license numbers or state identification numbers;

c. medical and/or health information.

31. Defendant had a duty to adopt reasonable measures to protect Plaintiffs' and Class Members' Private Information from involuntary disclosure to third parties.

32. In the untitled letter (the "Notice Letter") sent to Plaintiffs and Class Members, Defendant asserts that—on an unspecified date—SLT Lending "identified unusual activity in our network that caused certain devices to become unavailable."[5] In response, Defendant "immediately implemented our incident response plan, took steps to contain the activity, and launched an investigation."[6] As a result of that investigation, Defendant concluded—on May 11, 2023—that "an unauthorized actor accessed certain folders on our devices between March 15, 2023, and March 25, 2023[,]" including Plaintiffs' and Class Members' names, driver's license numbers or state identification numbers, and medical or health information.

33. Omitted from the Notice Letter were the details of the date that Defendant detected the Data Breach, the root cause of the Data Breach, the vulnerabilities exploited, and

[5] The "Notice Letter". A sample copy is available at https://apps.web.maine.gov/online/aeviewer/ME/40/9267a066-024b-41de-a5f7-d871fe00cd97.shtml (last accessed June 5, 2023)
[6] *Id.*

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 Plaintiffs and Class Members, who retain a vested interest in ensuring that their Private Information remains protected.

34. Upon information and belief, the cyberattack was targeted at Defendant, due to its status as an employer that collects, creates, and maintains Private Information on its computer networks and/or systems.

35. Upon information and belief, Plaintiffs' and Class Members' unencrypted Private Information was, in fact, acquired by unauthorized parties in the Data Breach.

36. The files, containing Plaintiffs' and Class Members' Private Information and stolen from Defendant, included the following: names, driver's license numbers, and medical and/or health information.[7]

37. Because of this targeted cyberattack, data thieves were able to gain access to and obtain data from Defendant that included the Private Information of Plaintiffs and Class Members.

38. As evidenced by the Data Breach's occurrence, the Private Information contained in Defendant's network was not encrypted. Had the information been properly encrypted, the data thieves would have exfiltrated only unintelligible data.

39. Plaintiffs' Private Information was accessed and stolen in the Data Breach and Plaintiffs believe their stolen Private Information is currently available for sale on the dark web because that is the *modus operandi* of cybercriminals.

[7] *Id.*

40. Due to the actual and continuing risk of identity theft as a result of the Data Breach, Plaintiffs and Class Members must, as Defendant's Notice Letter encourages them to do, monitor their financial accounts for many years to mitigate the risk of identity theft.[8]

41. In the Notice Letter, Defendant makes an offer of 12 months of identity monitoring services. This is wholly inadequate to compensate Plaintiffs and Class Members as it fails to provide for the fact that victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft, medical and financial fraud, and it entirely fails to provide sufficient compensation for the unauthorized release and disclosure of Plaintiffs' and Class Members' Private Information.

42. That Defendant is encouraging its current and former employees to enroll in credit monitoring and identity theft restoration services is an acknowledgment that the impacted individuals' Private Information *was* accessed, thereby subjecting Plaintiffs and Class Members to a substantial and continuing threat of fraud and identity theft.

43. Defendant had obligations created by the FTC Act, contract, state and federal law, common law, and industry standards to keep Plaintiffs' and Class Members' Private Information confidential and to protect it from unauthorized access and disclosure.

Data Breaches Are Preventable

44. Defendant could have prevented this Data Breach by, among other things, properly encrypting or otherwise protecting their equipment and computer files containing Private Information.

45. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive information they were maintaining for Plaintiffs and Class

[8] *Id.*

Members, causing the exposure of Private Information, such as encrypting the information or deleting it when it is no longer needed.

46. The unencrypted Private Information of 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 Private Information for targeted marketing without the approval of Plaintiffs and Class Members. Unauthorized individuals can easily access the Private Information of Plaintiffs and Class Members.

47. 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."[9]

48. 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 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.

[9] 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 Oct. 17, 2022).

- 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.[10]

49. To prevent and detect cyber-attacks or ransomware attacks UBMC 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;

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

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]

50. Given that Defendant was storing the Private Information of its current and former employees, Defendant could and should have implemented all of the above measures to prevent and detect cyberattacks.

51. 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 Private Information of tens of thousands of current and former employees, including Plaintiffs and Class Members.

[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).

Defendant Acquires, Collects, And Stores Employees' Private Information

52. Defendant acquires, collects, and stores a massive amount of Private Information on its employees, former employees and other personnel.

53. As a condition of employment, or as a condition of receiving certain benefits, Defendant requires that employees, former employees and other personnel entrust it with highly sensitive personal information.

54. By obtaining, collecting, and using Plaintiffs' and Class Members' Private Information, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiffs' and Class Members' Private Information from disclosure.

55. Plaintiffs and the Class Members have taken reasonable steps to maintain the confidentiality of their Private Information.

56. Plaintiffs and the Class Members relied on Defendant to keep their Private Information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

Defendant Knew or Should Have Known of the Risk Because Employers In Possession Of PII and PHI Are Particularly Suspectable To Cyber Attacks

57. 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 Private Information, like Defendant, preceding the date of the breach.

58. Data breaches, including those perpetrated against employers that store Private Information in their systems, have become widespread.

59. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.[12]

60. 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 Private Information are "attractive to ransomware criminals…because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[13]

61. In light of recent high profile data breaches at 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 the Private Information that they collected and maintained would be targeted by cybercriminals.

62. Defendant knew and understood that unprotected or exposed Private Information in the custody of employers, like Defendant, is valuable and highly sought after by nefarious third parties seeking to illegally monetize that Private Information through unauthorized access.

---

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

[13] 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).

63. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the Private Information of Plaintiffs 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 Plaintiffs and Class Members as a result of a breach.

64. Plaintiffs 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 Private Information.

65. The injuries to Plaintiffs and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the Private Information of Plaintiffs and Class Members.

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

67. As a business in custody of current and former employees' Private Information, Defendant knew, or should have known, the importance of safeguarding Private Information entrusted to them by Plaintiffs and Class Members, and of the foreseeable consequences if its data security systems were breached. This includes the significant costs imposed on Plaintiffs and Class Members as a result of a breach. Defendant failed, however, to take adequate cybersecurity measures to prevent the Data Breach.

Value Of Private Information

68. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without

authority."[14] 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."[15]

69. 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 credentials.[16]

70. For example, Personal Information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[17]

71. Criminals can also purchase access to entire company data breaches from $900 to $4,500.[18]

72. Driver's license numbers, which were compromised in the Data Breach, are incredibly valuable. "Hackers harvest license numbers because they're a very valuable piece of information.

[14] 17 C.F.R. § 248.201 (2013).
[15] *Id.*
[16] *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).
[17] *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).
[18] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last visited Oct. 217, 2022).

73. 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."[19]

74. 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.

75. 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 piece of information to lose if it happens in isolation."[20] 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."[21]

---

[19] https://www.forbes.com/sites/leemathews/2021/04/20/hackers-stole-customers-license-numbers-from-geico-in-months-long-breach/?sh=3e4755c38658 (last visited on Feb. 21, 2023).

[20] https://www.cpomagazine.com/cyber-security/geico-data-breach-leaks-drivers-license-numbers-advises-customers-to-watch-out-for-fraudulent-unemployment-claims/ (last visited on Feb. 21, 2023).

[21] *Id.*

76. Victims of driver's license number theft also often suffer unemployment benefit fraud, as described in a recent New York Times article.[22]

77. 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—name and medical information.

78. 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 . . . [is] worth more than 10x on the black market."[23]

79. 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.

80. 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 Private Information 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

[22] *How Identity Thieves Took My Wife for a Ride,* NY Times, April 27, 2021, available at: https://www.nytimes.com/2021/04/27/your-money/identity-theft-auto-insurance.html (last visited on Feb. 21, 2023).

[23] Tim 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).

> 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.[24]

Defendant Fails To Comply With FTC Guidelines

81. 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.

82. 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 employee information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[25]

83. 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.[26]

84. The FTC further recommends that companies not maintain Private Information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor

---

[24] *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).
[25] *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).
[26] *Id.*

for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

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

86. These FTC enforcement actions include actions against employers over the compromised Private Information of its employees, like Defendant here.

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

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

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

Defendant Fails To Comply With Industry Standards

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

91. Several best practices have been identified that a minimum should be implemented by employers in possession of Private Information, 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.

92. Other best cybersecurity practices that are standard for employers 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.

93. 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.

94. These foregoing frameworks are existing and applicable industry standards for an employer's obligations to provide adequate data security for its employees. 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

95. As a result of Defendant's ineffective and inadequate data security practices, the Data Breach, and the foreseeable consequences of Private Information ending up in the possession of criminals, the risk of identity theft to the Plaintiffs and Class Members has materialized and is imminent, and Plaintiffs and Class Members have all sustained actual injuries and damages, including: (a) invasion of privacy; (b) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (c) the loss of benefit of the bargain (price premium damages); (d) diminution of value of their Private Information; and (e) the continued risk to their Private Information, 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 Plaintiffs' and Class Members' Private Information.

The Data Breach Increases Victims' Risk Of Identity Theft

96. Plaintiffs and Class Members are at a heightened risk of identity theft for years to come.

97. The unencrypted Private Information of Class Members will end up for sale on the dark web because that is the *modus operandi* of hackers. In addition, unencrypted Private Information may fall into the hands of companies that will use the detailed Private Information for targeted marketing without the approval of Plaintiffs and Class Members. As a result of the Data Breach, unauthorized individuals can easily access the Private Information of Plaintiffs and Class Members.

98. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal Private Information 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.

99. 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 ident—y--or track the victim to attempt other hacking crimes against the individual to obtain more data to perfect a crime.

100. 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.

101. One such example of criminals piecing together bits and pieces of compromised Private Information for profit is the development of "Fullz" packages.[27]

[27] "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off of those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See*, *e.g.*, Brian Krebs, *Medical Records for Sale in Underground Stolen From Texas Life Insurance Firm*, Krebs on Security (Sep. 18, 2014), https://krebsonsecuritv.eom/2014/09/medical-records-for-sale-in-underground-stolen-

102. With "Fullz" packages, cyber-criminals can cross-reference two sources of Private Information to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals.

103. The development of "Fullz" packages means here that the stolen Private Information from the Data Breach can easily be used to link and identify it to Plaintiffs' and Class Members' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the Private Information that was exfiltrated in the Data Breach, criminals may still easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

104. The existence and prevalence of "Fullz" packages means that the Private Information stolen from the data breach can easily be linked to the unregulated data (like phone numbers and emails) of Plaintiffs and the other Class Members.

105. Thus, even if certain information (such as emails or telephone numbers) was not stolen in the data breach, criminals can still easily create a comprehensive "Fullz" package.

106. Then, this comprehensive dossier can be sold—and then resold in perpetuity—to crooked operators and other criminals (like illegal and scam telemarketers).

Loss Of Time To Mitigate 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 Private Information was compromised,

---

from-texas-life-insurance-](https://krebsonsecuritv.eom/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-finn/ (last visited on May 26, 2023).

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, Plaintiffs and Class Members must, as Defendant's Notice Letter encourages them to do, monitor their financial accounts for many years to mitigate the risk of identity theft.

109. Plaintiffs and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions, such as enrolling in the credit monitoring and identity theft insurance offered by defendant, contacting credit bureaus to place freezes on their accounts, contacting banks regarding fraudulent charges, and contacting the Social Security Administration to further secure their accounts.

110. Plaintiffs' 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."[28]

111. Plaintiffs' 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

[28] *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.

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.[29]

112. 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."[30]

Diminution Value Of PII and PHI

113. PII and PHI are valuable property rights.[31] Their 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 Private Information has considerable market value.

114. For example, drug manufacturers, medical device manufacturers, pharmacies, hospitals and other entities in custody of PHI often purchase Private Information on the black market for the purpose of target marketing their products and services to the physical maladies of the data breach victims themselves. Insurance companies purchase and use wrongfully disclosed Private Information to adjust their insureds' medical insurance premiums.

---

[29] *See* Federal Trade Commission, *Identity Theft.gov*, https://www.identitytheft.gov/Steps (last visited July 7, 2022).

[30] *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").

[31] *See, e.g.,* Brian T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("Private Information") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("Private Information, 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).

115. An active and robust legitimate marketplace for PII exists. In 2019, the data brokering industry was worth roughly $200 billion.[32]

116. 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.[33,34]

117. Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.[35]

118. Sensitive Private Information can sell for as much as $363 per record according to the Infosec Institute.[36]

119. As a result of the Data Breach, Plaintiffs' and Class Members' Private Information, 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 Plaintiffs or Class Members for their property, resulting in an economic loss. Moreover, the Private Information is now readily available, and the rarity of the Data has been lost, thereby causing additional loss of value.

120. 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

[32] https://www.latimes.com/business/story/2019-11-05/column-data-brokers
[33] https://datacoup.com/
[34] https://digi.me/what-is-digime/
[35] Nielsen Computer & Mobile Panel, Frequently Asked Questions, available at https://computermobilepanel.nielsen.com/ui/US/en/faqen.html
[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).

information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change, e.g., names, medical information, and health information.

121. 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.

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

123. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the Private Information of Plaintiffs 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 Plaintiffs and Class Members as a result of a breach.

124. 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 tens 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.

125. The injuries to Plaintiffs and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the Private Information of Plaintiffs and Class Members.

Future Cost Of Credit And Identity Theft Monitoring Is Reasonable And Necessary

126. Given the type of targeted attack in this case and sophisticated criminal activity, the type of Private Information involved, and the volume of data obtained in the Data Breach, 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 Private Information 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.

127. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that his or her Private Information 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.

128. Furthermore, the information accessed and disseminated in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, where victims can easily cancel or close credit and debit card accounts, because the information disclosed in this Data Breach is impossible to "close" and difficult, if not impossible, to change (such as name and medical information).

129. Consequently, Plaintiffs and Class Members are at a present and continuous risk of fraud and identity theft for many years into the future.

130. The retail cost of credit monitoring and identity theft monitoring can cost around $200 a year per Class Member. This is a 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 Plaintiffs and Class Members would not need to bear but for Defendant's failure to safeguard their Private Information.

Loss Of The Benefit Of The Bargain

131. Furthermore, Defendant's poor data security deprived Plaintiffs and Class Members of the benefit of their bargain. When submitting Private Information to Defendant

under certain terms through a job application and/or onboarding paperwork, Plaintiffs and other reasonable employees understood and expected that Defendant would properly safeguard and protect their Private Information, when in fact, Defendant did not provide the expected data security. Accordingly, Plaintiffs and Class Members received an employment position of a lesser value than what they reasonably expected to receive under the bargains they struck with Defendant.

PLAINTIFFS' EXPERIENCES

Plaintiff Brian Baker

132. More than ten years ago, Plaintiff Baker was employed at SLT Lending.

133. In the course of enrolling in employment with Defendant and as a condition of employment, he was required to supply Defendant with his Private Information.

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

135. At the time of the Data Breach, between March 15, 2023 and March 25, 2023, Defendant retained Plaintiff's Private Information in its system despite no longer maintaining an employment relationship with Plaintiff for *more than a decade.*

136. Plaintiff Baker received the Notice Letter, by U.S. mail, directly from Defendant, dated May 24, 2023. According to the Notice Letter, Plaintiff's Private Information was improperly accessed and obtained by unauthorized third parties, including his full name, driver's license number or state identification number, and medical and/or health information.

137. Upon receiving the Notice Letter form Defendant, Plaintiff Baker has spent significant time dealing with the consequences of the Data Breach including enrolling in the credit monitoring and identity theft insurance offered by defendant, contacting credit bureaus to place freezes on their accounts, contacting banks regarding fraudulent charges, and contacting the Social Security Administration to further secure their accounts. Plaintiff has spent significant time—at least 7 to 8 hours, at this time—in response to the Data Breach. This is valuable time that is forever lost and cannot be recaptured.

138. Subsequent to and as a result of the Data Breach, Plaintiff Baker has suffered numerous, substantial injuries including, but not limited to: (i) two fraudulent charges, totaling approximately $900, to his Wells Fargo debit card in March 2023; (ii) an increase in spam calls, texts, and/or emails; (iii) lost or diminished value of his Private Information; (iv) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; (v) invasion of privacy; and (vi) the continued and certainly increased risk to his Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains 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 Private Information.

139. Plaintiff Baker additionally suffered actual injury and damages as a result of the Data Breach. Implied in his employment contract with Defendant was the requirement that it adequately safeguard his Private Information and that it would delete or destroy his Private Information after Defendant was no longer required to retain it. Plaintiff Baker would not have worked for Defendant had Defendant disclosed that it lacked data security practices adequate to safeguard Private Information.

140. Plaintiff Baker further suffered actual injury in the form of damages and diminution in the value of his Private Information —a form of intangible property that he entrusted to Defendant for the purpose of employment, which was compromised by the Data Breach.

141. Plaintiff Baker also suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of his privacy, especially his medical and health information, being in the hands of criminals.

142. Plaintiff Baker has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his stolen Private Information being placed in the hands of unauthorized third parties and possibly criminals.

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

Plaintiff Luann Petrulakis

144. Plaintiff Luann Petrulakis is a former employee of Defendant. As a condition of employment with Defendant, Plaintiff Petrulakis was required to give her Private Information to Defendant.

145. Plaintiff Petrulakis is very careful about sharing her Private Information. She has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Plaintiff Petrulakis stores any documents containing her Private Information in a safe and secure location or destroys any such documents.

146. Plaintiff Petrulakis only allowed Defendant to maintain, store, and use her Private Information because she believed that Defendant would use basic, industry standard data security measures, such as those set forth herein, to protect it from unauthorized access.

147. Plaintiff Petrulakis received the Notice of Data Breach on or around June 1, 2023 which states, in relevant part, that her name, driver's license number or state identification number, and/or medical or health information were disclosed in the Data Breach.

148. As a result of the Data Breach, Plaintiff Petrulakis made reasonable efforts to mitigate the impact of the Data Breach after receiving the data breach notification, including but not limited to researching the Data Breach and reviewing financial reports and financial account statements for any indications of actual or attempted identity theft or fraud. Plaintiff Petrulakis has spent several hours dealing with the Data Breach; valuable time Plaintiff Petrulakis otherwise would have spent on other activities, including but not limited to recreation. Plaintiff and Class Members will need identity theft protection services and credit monitoring services for their respective lifetimes, considering the immutable nature of the PHI and PII at issue, which includes driver's license numbers and medical information. This time, which has been lost forever and cannot be recaptured, was spent at Defendant's direction.

149. As a result of the Data Breach, Plaintiff Petrulakis has suffered emotional distress as a result of the release of her Private Information, which she believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using her Private Information for purposes of identity theft and fraud. Plaintiff Petrulakis is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

150. Plaintiff Petrulakis suffered actual injury from having her Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of her Private Information, a form of tangible property that Defendant obtained from Plaintiff Petrulakis; (b) violation of her privacy rights; and (c) present, imminent

and impending injury arising from the increased risk of identity theft, fraud, and misuse resulting from her Private Information being placed in the hands of criminals.

151. As a result of the Data Breach, Plaintiff Petrulakis 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 Petrulakis will continue to be at substantial and immediate risk of identity theft and fraud for years to come.

Plaintiff Jamelah Elder

152. Plaintiff Elder was required to provide her Private Information to Defendant in connection with her being an employee of Defendant in or around 2014 at their San Francisco location and again in 2017 when she was rehired at a different location in Pasadena, CA. Plaintiff Elder has not been an employee for Defendant for approximately five years.

153. Plaintiff Elder is very careful about sharing her Private Information. Plaintiff Elder has never knowingly transmitted unencrypted sensitive PHI or PII over the internet or any other unsecured source. Plaintiff Elder stores any documents containing her sensitive PHI and PII in a safe and secure location or destroys the documents. Moreover, Plaintiff Elder diligently chooses unique usernames and passwords for her various online accounts.

154. Plaintiff Elder only allowed Defendant to maintain, store, and use her Private Information because she believed that Defendant would use adequate security measures to protect her Private Information, such as requiring passwords and multi-factor authentication to access databases storing her Private Information. As a result, Plaintiff Elder's Private Information was within the possession and control of Defendant at the time of the Data Breach.

155. In or around May 2023, Plaintiff Elder received notice from Defendant that her Private Information had been improperly accessed during a cybersecurity incident in March

2023. Defendant notified Plaintiff and Class members that "an unauthorized actor accessed certain folders on [its] devices between March 15, 2023 and March 25, 2023" and obtained Plaintiff's and Class Members' "name[s], driver's license number[s] or state identification number[s], and/or medical or health information." There is no indication from Defendant that the PHI and PII was encrypted or redacted in any way.

156. As a result of the Data Breach, Plaintiff Elder made reasonable efforts to mitigate the impact of the Data Breach after receiving the data breach notification, 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; researching the credit monitoring and identity theft protection services offered by Defendant; checking her credit monitoring service. Plaintiff Elder has spent at least five hours dealing with the Data Breach; valuable time Plaintiff Elder otherwise would have spent on other activities, including but not limited to recreation. Plaintiff and Class Members will need identity theft protection services and credit monitoring services for their respective lifetimes, considering the immutable nature of the PHI and PII at issue, which includes driver's license numbers and medical information. This time, which has been lost forever and cannot be recaptured, was spent at Defendant's direction.

157. As a result of the Data Breach, Plaintiff Elder has suffered emotional distress as a result of the release of her Private Information, which she believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using her Private Information for purposes of identity theft and fraud. Plaintiff Elder is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

158. Plaintiff Elder suffered actual injury from having her Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of her Private Information, a form of tangible property that Defendant obtained from Plaintiff Elder; (b) violation of her privacy rights; and (c) present, imminent and impending injury arising from the increased risk of identity theft, fraud, and misuse resulting from her Private Information being placed in the hands of criminals.

159. As a result of the Data Breach, Plaintiff Elder 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 Elder will continue to be at substantial and immediate risk of identity theft and fraud for years to come.

160. Defendant acknowledged the risk posed to Plaintiff Elder and her Private Information. Indeed, Defendant offered a one-year credit monitoring service.

161. As a result of the Data Breach, Plaintiff and Class Members are at an imminent, immediate, and continuing increased risk of experiencing devastating instances of identity theft, including but not limited to, having medical services and/or prescriptions ordered and obtained in their names, loans opened in their names, tax returns filed in their names, utility bills opened in their names, credit card accounts opened in their names, unauthorized charges made on their financial accounts, and other forms of identity theft.

162. Plaintiff and Class Members also face a substantial risk of being targeted in future phishing, data intrusion, and other illegal schemes through the misuse of their Private Information, since potential fraudsters will likely use such Private Information to continue to carry out such targeted schemes against Plaintiff and Class Members.

163. The Private Information maintained by and stolen from Defendant's systems, combined with publicly available information, allows nefarious actors to assemble a detailed mosaic of Plaintiff and Class Members, which has been and will continue to be used to carry out targeted fraudulent schemes against Plaintiff and Class Members.

164. Further, as a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been forced to spend time dealing with the effects of the Data Breach. Specifically, Plaintiff and Class Members have also been forced to take the time and effort to mitigate the actual and potential impact of the data breach on their everyday lives, including placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts, credit reports, and explanations of benefits for unauthorized activity for years to come.

165. Plaintiff and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

166. Plaintiff and Class Members also suffered a loss of value of their Private Information when it was acquired by cyber criminals in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases. Indeed, an active and robust legitimate marketplace for Private Information 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 sell their non-public information directly to a data broker who in turn aggregates the

[37] *See* Data Coup, https://datacoup.com/ (last visited on May 30, 2023).

information and provides it to other companies. Consumers who agree to provide their web browsing history to the Nielsen Corporation, for example, can in turn receive up to $50 a year.[38]

167. As a result of the Data Breach, Plaintiff's and Class Members' Private Information, which has an inherent market value in both legitimate and illegal markets, has been harmed and diminished due to its acquisition by cybercriminals. This transfer of valuable information happened with no consideration paid to Plaintiff or Class Members for their property, resulting in an economic loss. Moreover, the Private Information is apparently readily available to others, and the rarity of the Private Information has been destroyed because it is no longer only held by Plaintiff and the Class Members, and because that data no longer necessarily correlates only with activities undertaken by Plaintiff and the Class Members, thereby causing additional loss of value.

168. Further, Plaintiff and Class Members lost the benefit of their bargain with Defendant when they turned over their Private Information to Defendant as required under certain terms of their employment with Defendant. Plaintiff and Class Members, as reasonable employees, understood and expected that Defendant would properly safeguard and protect their Private Information when, in fact, Defendant did not provide the expected data security. Accordingly, Plaintiff and Class Members received an employment position of a lesser value than what they reasonably expected to receive under the bargains they struck with Defendant.

169. Finally, Plaintiff and Class Members have suffered or will suffer actual injury as a direct and proximate result of the Data Breach in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach. These losses include, but are not limited to, monitoring for and discovering fraudulent charges and/or medical

[38] *Frequently Asked Questions,* Nielsen Computer & Mobile Panel, https://computermobilepanel.nielsen.com/ui/US/en/faqen.html (last visited May 30, 2023).

identity theft and the stress, nuisance, and aggravation of dealing with all other issues resulting from the Data Breach.

170. Moreover, Plaintiff and Class Members have an interest in ensuring that their Private Information, which is believed to still be in the possession of SLT Lending, is protected from future additional breaches by the implementation of more adequate data security measures and safeguards, including but not limited to, ensuring that the storage of data or documents containing personal and financial information is not accessible online, that access to such data is password-protected, and that such data is properly encrypted.

171. As a direct and proximate result of SLT Lending's actions and inactions, Plaintiff and Class Members have suffered a loss of privacy and have suffered cognizable harm, including an imminent and substantial future risk of harm, in the forms set forth above.

172. Both Plaintiff and Class Members now face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

173. Plaintiff and Class Members have been and face a substantial risk of being targeted in the future, subjected to phishing, data intrusion, and other illegal actions based on their Private Information as potential fraudsters could use that information to target such schemes more effectively.

174. Plaintiff and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the cyber-attack.

175. Plaintiff and Class Members have spent and will continue to spend significant amounts of time to monitor their financial and medical accounts and records for misuse.

176. Plaintiff and Class Members have suffered or will suffer actual injury as a direct result of the cyber-attack. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the cyber-attack relating to:

a. Finding fraudulent charges;

b. Canceling and reissuing credit and debit cards;

c. Purchasing credit monitoring and identity theft prevention;

d. Addressing their inability to withdraw funds linked to compromised accounts;

e. Taking trips to banks and waiting in line to obtain funds held in limited accounts;

f. Placing "freezes" and "alerts" with credit reporting agencies;

g. Spending time on the phone with or at a financial institution to dispute fraudulent charges;

h. Contacting financial institutions and closing or modifying financial accounts;

i. Resetting automatic billing and payment instructions from compromised credit and debit cards to new ones;

j. Paying late fees and declined payment fees imposed as a result of failed automatic payments that were tied to compromised cards that had to be cancelled; and

k. Closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

177. Moreover, Plaintiff and Class Members have an interest in ensuring that their Private Information, which remains in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards, including but not limited

to, making sure that the storage of data or documents containing personal and financial information is not accessible online and that access to such data is password-protected.

178. Further, as a result of Defendant's conduct, Plaintiff and Class Members are forced to live with the anxiety that their Private Information—which contains the most intimate details about a person's life—may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

179. Plaintiff and Class Members were also injured and damaged by the delayed notice of this data breach, as it exacerbated the substantial and present risk of harm by leaving Plaintiff and Class Members without the knowledge that would have enabled them to take proactive steps to protect themselves.

180. As a direct and proximate result of Defendant's actions and inactions, Plaintiff and Class Members have suffered anxiety, emotional distress, and loss of privacy, and are at a present and definitely increased risk of future harm.

CLASS ACTION ALLEGATIONS

181. Plaintiffs bring this action on behalf of themselves and on behalf of all other persons similarly situated.

182. Pursuant to Federal Rule of Civil Procedure 23, Plaintiffs propose the following Class definition, subject to amendment as appropriate:

> **Nationwide Class**
> All persons in the United States whose Private Information was maintained on Defendant's computer systems that were compromised in the Data Breach announced by Defendant in May 2023 (the "Class").

183. Additionally, Plaintiff Elder proposes the following California Subclass definition, subject to amendment as appropriate:

California Subclass
All persons in the State of California whose Private Information was maintained on Defendant's computer systems that were compromised in the Data Breach announced by Defendant in May 2023 (the "California Subclass").

184. Similarly, Plaintiff Petrulakis proposes the following Illinois Subclass definition, subject to amendment as appropriate:

Illinois Subclass
All persons in the State of Illinois whose Private Information was maintained on Defendant's computer systems that were compromised in the Data Breach announced by Defendant in May 2023 (the "Illinois Subclass").

185. Excluded from the Classes are Defendant's officers and directors, and any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Class are members of the judiciary to whom this case is assigned, their families and members of their staff.

186. Plaintiffs hereby reserve the right to amend or modify the Class definition with greater specificity or division after having had an opportunity to conduct discovery.

187. Numerosity. The Members of the Class are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiffs at this time, based on information and belief, according to the report submitted to the Maine Attorney General, the Class consists at least 40,000 persons whose data was compromised in Data Breach.[39]

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

[39] *See* https://apps.web.maine.gov/online/aeviewer/ME/40/9267a066-024b-41de-a5f7-d871fe00cd97.shtml (last accessed June 5, 2023)

a. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiffs' and Class Members' Private Information;

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

c. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

d. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

e. Whether Defendant owed a duty to Class Members to safeguard their Private Information;

f. Whether Defendant breached its duty to Class Members to safeguard their Private Information;

g. Whether computer hackers obtained Class Members' Private Information in the Data Breach;

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

i. Whether Plaintiffs and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;

j. Whether Defendant's conduct was negligent;

k. Whether Defendant breached implied contracts for adequate data security with Plaintiffs and Class Members;

l. Whether Defendant was unjustly enriched by retention of the monetary benefits conferred on it by Plaintiffs and Class Members;

m. Whether Defendant failed to provide notice of the Data Breach in a timely manner; and,

n. Whether Plaintiffs and Class Members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

189. Typicality. Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' Private Information, like that of every other Class Member, was compromised in the Data Breach.

190. Adequacy of Representation. Plaintiffs will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiffs' Counsel are competent and experienced in litigating class actions.

191. Predominance. Defendant has engaged in a common course of conduct toward Plaintiffs and Class Members, in that all the Plaintiffs' and Class Members' Private Information was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

192. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual

Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

193. 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.

194. Likewise, particular issues under Fed. R. Civ. P. 23(c)(4) 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 owed a legal duty to Plaintiffs and the Class to exercise due care in collecting, storing, and safeguarding their Private Information;

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

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

d. Whether Defendant failed to take commercially reasonable steps to safeguard consumer Private Information; and

e. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

195. Finally, all Members of the proposed Class are readily ascertainable. Defendant has access to Class Members' names and addresses affected by the Data Breach. Class Members have already been preliminarily identified and sent Notice of the Data Breach by Defendant.

COUNT I – Negligence
(By Plaintiffs on behalf of the Class)

196. Plaintiffs restate and reallege all proceeding allegations above and hereafter as if fully set forth herein.

197. This count is brought on behalf of all Class Members.

198. Defendant required Plaintiffs and Class Members to submit non-public Private Information as a condition of employment or as a condition of receiving employee benefits.

199. Plaintiffs and the Class Members entrusted their Private Information to Defendant with the understanding that Defendant would safeguard their information and delete it once the employment relationship terminated.

200. By assuming the responsibility to collect and store this data, and in fact doing so, 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 they could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

201. 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.

202. Section 5 of the FTC Act, as interpreted and enforced by the FTC, prohibits the unfair act or practice by businesses, such as Defendant,[40] of failing to use reasonable measures to protect Private Information. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant's duty to protect Plaintiffs and the members of the Class's sensitive Private Information.

203. Plaintiffs and members of the Class are within the class of persons that the FTC Act was intended to protect.

204. 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 employers, which, as a result of failures to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm to its employees as that suffered by Plaintiffs and members of the Class.

205. Defendant's conduct constitutes negligence *per se* because it was in violation of Section 5 of the FTC Act by failing to use reasonable measures to protect Private Information and not complying with applicable industry standards.

206. Defendant's conduct was particularly unreasonable given the nature and amount of Private Information it obtained and stored, and the foreseeable consequences of the Data Breach for companies of Defendant's magnitude, including, specifically, the immense damages that would result to Plaintiffs and Members of the Class due to the valuable nature of the Private Information at issue in this case—including their health and medical information.

[40] https://www.ftc.gov/news-events/news/press-releases/2011/05/ftc-settles-charges-against-two-companies-allegedly-failed-protect-sensitive-employee-data

207. 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.

208. Defendant breached its duties, and thus was 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:

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

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

c. Failing to periodically ensure that their email system had plans in place to maintain reasonable data security safeguards;

d. Allowing unauthorized access to Class Members' Private Information; and,

e. Failing to detect in a timely manner that Class Members' Private Information had been compromised.

209. 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 the industry.

210. 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.

211. There is a temporal and close causal connection between Defendant's failure to implement security measures to protect the Private Information and the harm suffered, or risk of imminent harm suffered by Plaintiffs and the Class.

212. As a result of Defendant's negligence, Plaintiffs and the Class Members have suffered and will continue to suffer damages and injury including, but not limited to: (i) Plaintiffs experiencing fraudulent charges to his debit card; (ii) lost or diminished value of their Private Information; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; (iv) invasion of privacy; (v) loss of benefit of the bargain; and (vi) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains 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 Private Information.

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

214. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to, *e.g.,* (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 the Class.

COUNT II – Negligence *Per Se*
(By Plaintiffs on behalf of the Class)

215. Plaintiffs restate and reallege all proceeding allegations above and hereafter as if fully set forth herein.

216. This count is brought on behalf of all Class Members.

217. Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by companies, such as Defendant, of failing to use reasonable measures to

protect Private Information. Various FTC publications and orders also form the basis of Defendant's duty.

218. The Indiana Disclosure of Security Breach Act ("IDSBA") requires that entities in possession of Private Information belonging to Indiana residents that was or may have been accessed by unauthorized persons disclose the data breach without unreasonable delay. *See* In. Stat. § 24-4.9- 1, *et seq.*

219. Defendant violated Section 5 of the FTC Act and IDSBA by failing to use reasonable measures to protect Private Information and not complying with industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of Private Information obtained and stored and the foreseeable consequences of a data breach on Defendant's systems.

220. Defendant's violation of Section 5 of the FTC Act and the IDSBA constitutes negligence *per se.*

221. Class Members are consumers within the class of persons Section 5 of the FTC Act and the IDSBA were intended to protect.

222. Moreover, the harm that has occurred is the type of harm the FTC Act and the IDSBA were intended to guard against. Indeed, the FTC has pursued over fifty 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 suffered by Plaintiffs and Class Members.

223. But for Defendant's wrongful and negligent breach of duties owed to Plaintiffs and the Class, the Private Information of Plaintiffs and the Class would not have been compromised.

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

225. As a direct and proximate result of Defendant's negligence *per se*, Plaintiffs and the Class have suffered and will suffer injury, including but not limited to: (i) Plaintiffs experiencing fraudulent charges to his debit card; (ii) lost or diminished value of their Private Information; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; (iv) invasion of privacy; (v) loss of benefit of the bargain; and (vi) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains 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 Private Information.

226. As a direct and proximate result of Defendant's negligence *per se*, Plaintiffs 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.

227. Additionally, as a direct and proximate result of Defendant's negligence *per se*, Plaintiffs and the Class have suffered and will suffer the continued risks of exposure of their Private Information, 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 Private Information in its continued possession.

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

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

230. Plaintiffs 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.

COUNT III – Breach of Implied Contract
(By Plaintiffs on behalf of the Class)

231. Plaintiffs restate and reallege all proceeding allegations above and hereafter as if fully set forth herein.

232. This count is brought on behalf of all Class Members.

233. Plaintiffs and Class Members were required to provide their Private Information to Defendant as a condition of their employment with Defendant.

234. Plaintiffs and Class Members provided their labor and their Private Information to Defendant in exchange for (among other things) Defendant's promise to protect their Private Information from unauthorized disclosure and to delete it once it was no longer necessary to maintain the Private Information for employment purposes. Defendant additionally promulgated, adopted, and implemented written privacy policies whereby it expressly promised Plaintiffs and Class Members that it would only disclose Private Information under certain circumstances, none of which relate to the Data Breach.

235. On information and belief, Defendant further promised to and represented it would comply with industry standards and to make sure that Plaintiffs' and Class Members' Private Information would remain protected.

236. Implicit in the agreement between Plaintiffs and Class Members and the Defendant to provide Private Information, was the latter's obligation to: (a) use such Private Information for business purposes only, (b) take reasonable steps to safeguard that Private Information, (c) prevent unauthorized disclosures of the Private Information, (d) provide Plaintiffs and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their Private Information, (e) reasonably safeguard and protect the Private Information of Plaintiffs and Class Members from unauthorized disclosure or uses, (f) retain the Private Information only under conditions that kept such information secure and confidential.

237. When Plaintiffs and Class Members provided their Private Information to Defendant as a condition of their employment or employee beneficiary status, they entered into implied contracts with Defendant pursuant to which Defendant agreed to reasonably protect such information.

238. Defendant required Class Members to provide their Private Information as part of Defendant's regular business practices. Plaintiffs and Class Members accepted Defendant's offers and provided their Private Information to Defendant.

239. In entering into such implied contracts, Plaintiffs and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations and were consistent with industry standards.

240. Plaintiffs and Class Members would not have entrusted their Private Information to Defendant in the absence of the implied contract between them and Defendant to keep their information reasonably secure.

241. Plaintiffs and Class Members would not have entrusted their Private Information to Defendant in the absence of its implied promise to monitor its computer systems and networks to ensure that it adopted reasonable data security measures.

242. Plaintiffs and Class Members fully and adequately performed their obligations under the implied contracts with Defendant.

243. Defendant breached its implied contracts with Class Members by failing to safeguard and protect their Private Information.

244. As a direct and proximate result of Defendant's breaches of the implied contracts, Class Members sustained damages as alleged herein.

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

246. Plaintiffs and Class Members are also entitled to nominal damages for the breach of implied contract.

247. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to, *e.g.*, (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to The Class.

Count IV – Unjust Enrichment
(By Plaintiffs on behalf of the Class)

248. Plaintiffs restate and reallege all proceeding allegations above and hereafter as if fully set forth herein.

249. This count is brought on behalf of all Class Members.

250. This count is pleaded in the alternative to Plaintiffs' breach of contract claim above (Count III).

251. Plaintiffs and Class Members conferred a monetary benefit upon Defendant in the form of their labor and by providing their valuable Private Information to Defendant.

252. Plaintiffs and Class Members provided Defendant their labor and Private Information on the understanding that Defendant would pay for the administrative costs of reasonable data privacy and security practices and procedures from the revenue it derived therefrom. In exchange, Plaintiffs and Class members should have received adequate protection and data security for such Private Information held by Defendant.

253. Defendant benefited from receiving Plaintiffs' and Class Members' labor and from receiving their Private Information through its ability to retain and use that information for its own benefit. Defendant understood and accepted this benefit.

254. Defendant knew Plaintiffs and Class members conferred a benefit which Defendant accepted. Defendant profited from these transactions and used the Private Information of Plaintiffs and Class Members for business purposes.

255. Because all Private Information provided by Plaintiffs and Class Members was similarly at risk from a foreseeable and targeted data breach, Defendant's obligation to safeguard the Private Information it collected from its employees was inherent to the employment relationship.

256. Defendant also understood and appreciated that Plaintiffs' and Class Members' Private Information was private and confidential, and its value depended upon Defendant maintaining the privacy and confidentiality of that information.

257. Defendant failed to provide reasonable security, safeguards, and protections to the Private Information of Plaintiffs and Class Members.

258. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' Private Information.

259. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead made calculated decisions to avoid its data security obligations at the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective security measures. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

260. Under the principles of equity and good conscience, Defendant should not be permitted to retain money belonging to Plaintiffs and Class Members, because Defendant failed to implement appropriate data management and security measures mandated by industry standards.

261. Defendant's enrichment at the expense of Plaintiffs and Class Members is and was unjust.

262. Defendant acquired the monetary benefit and Private Information through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

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

264. Plaintiffs and Class Members have no adequate remedy at law.

265. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will suffer injury as described herein.

266. Plaintiffs and the Class Members are entitled to restitution and disgorgement of all profits, benefits, and other compensation obtained by Defendant, plus attorneys' fees, costs, and interest thereon.

Count V – Violation of the Drivers' Privacy Protection Act ("DPPA")
18 U.S.C. § 2721, *et seq.*
(By Plaintiffs on behalf of the Class)

267. Plaintiffs restate and reallege all proceeding allegations above and hereafter, as if fully set forth herein, and brings this claim on behalf of themselves and the Class.

268. The DPPA provides that "[a] person who knowingly obtains, discloses or uses personal information, from a motor vehicle record, for a purpose not permitted under this chapter shall be liable to the individual to whom the information pertains." 18 U.S.C. § 2724.

269. Under the DPPA, "person" is defined as "an individual, organization, or entity." 18 U.S.C. 2725(2). Defendant is a "person" under the DPPA.

270. Further, the definition of "disclose" is "to make known or public" or "expose to view."[41] Defendant's voluntary action of exposing Plaintiff's and Class Members' PII constitutes a knowing disclosure. In particular, Defendant voluntarily disclosed Plaintiff's and Class Members' PII when it failed to adequately secure their PII on its systems. In doing so, unauthorized actors were able to access and obtain the PII of Plaintiff and Class Members for nefarious purposes.

[41] https://www.merriam-webster.com/dictionary/disclose (last accessed on June 2, 2023).

271. The DPPA also restricts the resale and redisclosure of personal information and requires authorized recipients to maintain records of each individual and the permitted purpose of the disclosure for a period of five years. 18 U.S.C. § 2721(c).

272. Under the DPPA, a "'motor vehicle record' means any record that pertains to a motor vehicle operator's permit, motor vehicle title, motor vehicle registration, or identification card issued by a department of motor vehicles.'" 18 U.S.C. § 2725(1). Drivers' license numbers are motor vehicle records and personal information under the DPPA. 18 U.S.C. § 2725(3); *see also Dahlstrom v. Sun-Times Media, LLC*, 777 F.3d 937, 943 (7th Cir. 2015).

273. Defendant obtained, used, disclosed, resold, and redisclosed motor vehicle records from their employees.

274. Defendant also obtained motor vehicle records directly from state agencies or through resellers who sell such records.

275. Defendant knowingly used motor vehicle records for uses not permitted by the statute, including sales, and marketing, among other impermissible uses.

276. Defendant knowingly and voluntarily configured and designed their computer systems and/or linked their respective public websites to systems and/or networks storing, maintaining, and/or obtaining Plaintiff's and Class Members' PII, which resulted in the disclosure of Plaintiff's and Class Members' PII to cybercriminals.

277. Defendant failed to use reasonable care in protecting Plaintiff's and Class Members' PII by installing substandard security measures that failed to protect it.

278. Further, Defendant had actual and/or constructive notice of the risk to Plaintiff's and the Class Members' PII because they should have been aware that failing to incorporate

basic security measures in the configuration and design of their systems would cause the improper disclosure of Plaintiff's and Class Members' PII.

279. During the period between March 15, 2023 and March 25, 2023, PII, including drivers' license numbers and other information from motor vehicle records, of Plaintiff and Class Members, were available to thieves and have been removed from Defendant's systems. Defendant knowingly used and disclosed and/or redisclosed Plaintiff's and Class Members' motor vehicle records and PII to thieves, which is not an authorized use permitted by the DPPA pursuant to 18 U.S.C. §§ 2724, 2721(b), and 2721(c).

280. As a result of the Data Breach, Plaintiff and putative Class Members are entitled to actual damages, liquidated damages, punitive damages, attorneys' fees and costs.

Count VI – Invasion of Privacy
(By Plaintiffs on behalf of the Class)

281. Plaintiffs restate and reallege all proceeding allegations above and hereafter, as if fully set forth herein, and brings this claim on behalf of themselves and the Class.

282. Plaintiff and Class Members had a legitimate expectation of privacy to their PHI and PII and were entitled to the protection of this information against disclosure to unauthorized third parties.

283. Defendant owed a duty to Plaintiff and Class Members to keep their PHI and PII confidential.

284. Defendant intentionally failed to protect and released to unknown and unauthorized third parties the non-redacted and non-encrypted PHI and PII of Plaintiff and Class Members.

285. Defendant allowed unauthorized and unknown third parties access to and examination of the PHI and PII of Plaintiff and Class Members, by way of Defendant's failure to protect the PHI and PII.

286. The unauthorized release to, custody of, and examination by unauthorized third parties of the PHI and PII of Plaintiff and Class Members is highly offensive to a reasonable person.

287. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiff and Class Members disclosed their PHI and PII to Defendant as part of their relationships with Defendant, but privately with an intention that the PHI and PII would be kept confidential and would be protected from unauthorized disclosure. Plaintiff and Class Members were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

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

289. Defendant acted with intention and a knowing state of mind when it permitted the Data Breach to occur because it was with actual knowledge that their information security practices were inadequate and insufficient.

290. Because Defendant acted with this knowing state of mind, it had notice and knew its inadequate and insufficient information security practices would cause injury and harm to Plaintiff and Class Members.

291. As a proximate result of the above acts and omissions of Defendant, PHI and PII of Plaintiff and Class Members was disclosed to third parties without authorization, causing Plaintiff and Class Members to suffer damages.

292. Unless and until enjoined and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and Class Members in that the PHI and PII maintained by Defendant can be viewed, distributed, and used by unauthorized persons for years to come. Plaintiff and Class Members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiff and Class Members.

Count VII – Violation of the California Consumer Privacy Act
Cal. Civ. Code §§ 1798.100, *et. seq*. ("CCPA")
(By Plaintiff Elder on behalf of the California Subclass)

293. Plaintiff Elder ("Plaintiff" for the purposes of this count) restates and realleges all proceeding allegations above and hereafter, as if fully set forth herein, and brings this claim on behalf of herself and the California Subclass (the "Class" for the purposes of this count).

294. As more personal information about consumers is collected by businesses, consumers' ability to properly protect and safeguard their privacy has decreased. Consumers entrust businesses with their personal information on the understanding that businesses will adequately protect it from unauthorized access and disclosure. The California Legislature explained: "The unauthorized disclosure of personal information and the loss of privacy can have devasting effects for individuals, ranging from financial fraud, identity theft, and unnecessary costs to personal time and finances, to destruction of property, harassment, reputational damage, emotional stress, and even potential physical harm."

295. As a result, in 2018, the California Legislature passed the CCPA, giving consumers broad protections and rights intended to safeguard their personal information. Among other things, the CCPA imposes an affirmative duty on businesses that maintain personal information about California residents to implement and maintain reasonable security procedures and practices that are appropriate to the nature of the information collected. Defendant failed to implement such procedures which resulted in the Data Breach.

296. It also requires "[a] business that discloses personal information about a California resident pursuant to a contract with a nonaffiliated third party . . . [to] require by contract that the third party implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure." Cal. Civ. Code § 1798.81.5(c).

297. Section 1798.150(a)(1) of the CCPA provides:

> Any consumer whose nonencrypted or nonredacted personal information, as defined [by the CCPA] is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business' violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for statutory or actual damages, injunctive or declaratory relief, and any other relief the court deems proper.

298. Plaintiff and the California Subclass Members are "consumer[s]" as defined by Civ. Code § 1798.140(g) because they are "natural person[s] who [are] California resident[s], as defined in Section 17014 of Title 18 of the California Code of Regulations, as that section read on September 1, 2017."

299. Defendant is a "business" as defined by Civ. Code § 1798.140(c) because Defendant:

a. is a "sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners";

b. "collects consumers' personal information, or on the behalf of which is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information";

c. does business in California; and

d. has annual gross revenues in excess of $25 million; annually buys, receives for the business' commercial purposes, sells or shares for commercial purposes, alone or in combination, the personal information of 100,000 or more consumers, households, or devices; or derives 50 percent or more of its annual revenues from selling consumers' personal information.

300. The Private Information taken in the Data Breach is personal information as defined by Civil Code § 1798.81.5(d)(1)(A) because it contains Plaintiff's and the California Subclass Members' unencrypted names and driver's license numbers among other information.

301. Plaintiff and the California Subclass's Private Information was subject to unauthorized access and exfiltration, theft, or disclosure because their Private Information, including name and contact information was wrongfully taken, accessed, and viewed by unauthorized third parties.

302. The Data Breach occurred as a result of Defendant's failure to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect Plaintiff's and the California Subclass Members' Private Information. Defendant failed to implement reasonable security procedures to prevent an attack on their

server or network, including its email system, by hackers and to prevent unauthorized access of Plaintiff's and California Subclass Members' PHI and PII as a result of this attack.

303. On June 5, 2023, Plaintiff provided Defendant with written notice of its violations of the CCPA, pursuant to Civil Code § 1798.150(b)(1). Defendant timely responded on July 5, 2023, but failed to fully address and cure the violations alleged in the letter and herein. Attached hereto as Exhibits A and B are true and correct copies of Plaintiff's written notice and Defendant's response thereto.

304. Defendant did not actually cure the noticed violations. Defendant asserted, without evidence or proof, that they "cured" the above failures to implement reasonable security procedures to prevent unauthorized access of Plaintiff's and California Subclass Members' PII through steps taken by Defendant "[u]pon learning of suspicious activity on its network." The post- attack actions that Defendant allegedly took did not retroactively cure the unauthorized access, as they provide no assurance that Plaintiff and California Subclass Members' PII was not viewed by—and/or is not still in the hands of—unauthorized third parties.

305. Furthermore, none of the steps Defendant asserts in its response demonstrates an actual cure of its failure to implement reasonable security measures to protect Plaintiff's and California Subclass Members' PII, as the steps Defendant asserts it has taken are not sufficient to protect Plaintiff's and California Subclass Members' PII into the future. For example, Defendant did not include basic but effective security measures, including two-factor authentication and/or encryption, in its response to this breach.

306. Defendant's response is wholly insufficient to demonstrate any "actual cure" of its failure to implement reasonable security to protect Plaintiff's and California Subclass Members' information.

307. As Defendant has not "actually cured" the violation, Plaintiff and the California Subclass seek statutory damages in an amount not less than one hundred dollars ($100) and not greater than seven hundred and fifty ($750) per consumer per incident, or actual damages, whichever is greater, as well as all monetary and non-monetary relief allowed by law, including actual financial losses, injunctive relief, reasonable attorneys' fees and costs, and statutory damages. *See* Cal. Civ. Code § 1798.150(a)(1)(A) & (b).

308. If Defendant fails to respond, or has not "actually" cured, or is unable to "actually cure" the violation within 30 days thereof, Plaintiff will amend this Complaint to seek all relief available under the CCPA including damages to be measured as the greater of actual damages or statutory damages in an amount up to seven hundred and fifty dollars ($750) per consumer per incident. *See* Cal. Civ. Code § 1798.150(a)(1)(A) & (b).

309. As a result of Defendant's failure to implement and maintain reasonable security procedures and practices that resulted in the Data Breach, Plaintiff seeks injunctive relief, including public injunctive relief, declaratory relief, and any other relief as deemed appropriate by the Court.

Count VIII – Violation of the California Customer Records Act ("CCRA")
Cal. Civ. Code §§ 1798.80, *et. seq.*
(By Plaintiff Elder on behalf of the California Subclass)

310. Plaintiff Elder ("Plaintiff" for the purposes of this count) restates and realleges all proceeding allegations above and hereafter, as if fully set forth herein, and brings this claim on behalf of herself and the California Subclass (the "Class" for the purposes of this count).

311. The California legislature enacted the California Customer Records Act ("CCRA") to "ensure that personal information about California residents is protected." Cal. Civ. Code § 1798.81.5.

312. The CCRA states that any business which "owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure." Cal. Civ. Code § 1798.81.5(b).

313. Under the CCRA, personal information includes "[a]n individual's first name or first initial and the individual's last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted: Social Security number, Driver's license number . . . [or] medical information."

314. The personal information compromised in the Data Breach includes information that meets this definition. The information was unencrypted and unredacted as evidenced by the fact that Defendant was required to provide notification letters under the laws of several states that require notification of unauthorized access to unencrypted and unredacted information.

315. Defendant failed to maintain reasonable data security procedures appropriate to the nature of the personal information. Accordingly, Defendant violated Cal. Civ. Code § 1798.81.5(b).

316. Plaintiff and the California Subclass were injured by Defendant's violation of Cal. Civ. Code § 1798.81.5(b) and seek damages pursuant to Cal. Civ. Code § 1798.84(b). Plaintiff and the California Subclass were injured in the various ways alleged herein. They

seek all monetary and non-monetary relief allowed by the CCRA to compensate for their various types of damages alleged herein.

317. Plaintiff and the California Subclass are also entitled to injunctive relief pursuant to Cal. Civ. Code § 1798.84(e), including substantial improvements to Defendant's data security systems.

Count IX – Violation of the California Unfair Competition Law ("UCL")
Cal. Bus. & Prof. Code §§ 17200, *et. seq.*
(By Plaintiff Elder on behalf of the California Subclass)

318. Plaintiff Elder ("Plaintiff" for the purposes of this count) restates and realleges all proceeding allegations above and hereafter, as if fully set forth herein, and brings this claim on behalf of herself and the California Subclass (the "Class" for the purposes of this count).

319. Plaintiff and Defendant are "persons" as defined by Cal. Bus. & Prof. Code § 17201.

320. The UCL prohibits "unlawful, unfair, or fraudulent business acts or practices."

321. By failing to take reasonable precautions to protect the PHI and PII of Plaintiff and the California Subclass, Defendant has engaged in "unlawful" and "unfair" business practices in violation of the UCL.

322. First, Defendant engaged in "unlawful" acts or practices because it violated multiple laws, including the California Consumer Privacy Act, Cal. Civ. Code § 1798, *et seq.*; California Customer Records Act, Cal. Civ. Code §§ 1798.80, *et seq.*; the FTC Act; and the common law, all as alleged herein.

323. Second, Defendant engaged in "unfair" acts or practices, including the following:

324. Defendant failed to implement and maintain reasonable data security measures to protect the California Subclass Members' PHI and PII. Defendant failed to identify foreseeable security risks and adequately maintain their data security in light of the known risk of cyber intrusions, especially in light of the highly sensitive nature of the information which Defendant stored. Defendant's conduct, with little if any social utility, is unfair when weighed against the harm to the California Subclass Members whose PHI and PII has been compromised.

325. Defendant's failure to implement and maintain reasonable data security measures was contrary to legislatively-declared public policy that seeks to protect consumers' personal information and ensures that entities entrusted with PHI and PII adopt appropriate security measures. These policies are reflected in various laws, including the CCPA (Cal. Civ. Code §§ 1798.100 *et seq.*); the FTC Act (15 U.S.C. § 45).

326. Defendant's failure to implement and maintain reasonable data security measures led to the substantial consumer injuries described herein. These injuries are not outweighed by countervailing benefits to consumers or competition. Moreover, because consumers could not have reasonably known of Defendant's inadequate data security, consumers could not have reasonably avoided the harms that Defendant's conduct caused.

327. As a direct and proximate result of Defendant's acts of unlawful and unfair practices and acts, Plaintiff and the California Subclass were injured and lost money or property, and suffered the various types of damages alleged herein.

328. The UCL states that an action may be brought by any person who has "suffered injury in fact and has lost money or property as a result of the unfair competition." Cal. Bus. & Prof. Code § 17204. Plaintiff and the California Subclass Members suffered injury in fact

and lost money or property, including in the form of the loss of value of their breached PHI and PII, as a result of Defendant's unfair competition as set forth herein. PHI and PII is valuable which is demonstrated by the fact that Defendant's business is built in part by managing the PHI and PII of the California Subclass.

329. Plaintiff and Class Members would not have entrusted their Private Information to Defendant or accepted employment with Defendant had they known that Defendant would fail to implement reasonable and adequate data security procedures.

330. Plaintiff and the California Subclass are entitled to injunctive relief to address Defendant's past and future acts of unfair competition.

331. Plaintiff and the California Subclass are entitled to restitution of money and property that Defendant obtained by means of unlawful, unfair, or fraudulent practices, and restitutionary disgorgement of all profits accruing to Defendant as a result of their unlawful and unfair business practices.

332. Plaintiff lacks an adequate remedy at law because the injuries here include an imminent risk of identity theft and fraud that can never be fully remedied through damages.

333. Further, if an injunction is not issued, Plaintiff and California Subclass Members will suffer irreparable injury. The risk of another such breach is real, immediate, and substantial. Plaintiff and the California Subclass lack an adequate remedy at law that will reasonably protect them against the risk of such further breach.

334. Plaintiff and the California Subclass seek all monetary and non-monetary relief available to them under the UCL, including reasonable attorney's fees as allowed under Cal. Code Civ. Proc. §1021.5.

Count X – Violation Of The Illinois Consumer Fraud Act
815 Ill. Comp. Stat. §§ 505/1, *et seq.*
(By Plaintiff Petrulakis on behalf of the Illinois Subclass)

335. Plaintiff Petrulakis ("Plaintiff" for the purposes of this count) restates and realleges all proceeding allegations above and hereafter, as if fully set forth herein, and brings this claim on behalf of herself and the Illinois Subclass (the "Class" for the purposes of this count).

336. Plaintiff and the Class are "consumers" as that term is defined in 815 ILL. COMP. STAT. § 505/1(e).

337. Plaintiff, the Class, and Defendant are "persons" as that term is defined in 815 ILL. COMP. STAT. § 505/1(c).

338. Defendant is engaged in "trade" or "commerce," including the provision of services, as those terms are defined under 815 ILL. COMP. STAT. § 505/1(f).

339. Defendant engages in the "sale" of "merchandise" (including services) as defined by 815 ILL. COMP. STAT. § 505/1(b) and (d).

340. Defendant's acts, practices, and omissions were done in the course of Defendant's business of marketing, offering for sale, and selling products and/or services in the State of Illinois.

341. Defendant engaged in deceptive and unfair acts and practices, misrepresentation, and the concealment, suppression, and omission of material facts in connection with the sale and advertisement of "merchandise" (as defined in the Illinois CFA) in violation of the Illinois CFA, including, but not limited to, the following:

a. failure to maintain adequate computer systems and data security practices to safeguard current and former customers' Private Information;

b. failure to disclose the material fact that its computer systems and data security practices were inadequate to safeguard the personal information it was collecting and maintaining from theft;

c. failure to disclose in a timely and accurate manner to Plaintiff and the Class Members the material fact of Defendant's data breach;

d. misrepresenting material facts to Plaintiff and the Class, in connection with the sale of goods and services, by representing that it would maintain adequate data privacy and security practices and procedures to safeguard Plaintiff's and Class members' Private Information from unauthorized disclosure, release, data breaches, and theft;

e. misrepresenting material facts to the class, in connection with the sale of goods and services, by representing that Defendant did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Plaintiff's and Class members' Private Information, and

f. failing to take proper action following the Data Breach to enact adequate privacy and security measures and protect Plaintiff's and Class members' Private Information from further unauthorized disclosure, release, data breaches, and theft.

342. In addition, Defendant's failure to disclose that its computer systems were not well protected and that Plaintiff's and Class members' sensitive information was vulnerable and susceptible to intrusion and cyberattacks constitutes deceptive and/or unfair acts or practices because Defendant knew such facts would (a) be unknown to and not easily discoverable by Plaintiff and the Class; and (b) defeat Plaintiff's and Class members' ordinary,

foreseeable and reasonable expectations concerning the security of their Private Information on Defendant's servers.

343. Defendant intended that Plaintiff and the Class rely on its deceptive and unfair acts and practices, misrepresentations, and the concealment, suppression, and omission of material facts, in connection with Defendant's offering of goods and services and storing Plaintiff's and Class members' Private Information on its servers, in violation of the Illinois CFA.

344. Defendant also engaged in unfair acts and practices by failing to maintain the privacy and security of class members' personal information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the data breach.

345. These unfair acts and practices violated duties imposed by laws including Section 5 of the Federal Trade Commission Act (15 U.S.C. § 45) and similar state laws.

346. Defendant's duties also arise from the Illinois Personal Information Protection Act ("IPIPA"), 815 Ill. Comp. Stat. § 530/45(a) which requires:

> A data collector that owns or licenses, or maintains or stores but does not own or license, records that contain personal information concerning an Illinois resident shall implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification, or disclosure.

815 ILCS 530/45. LSSI violated this duty by failing to implement reasonably secure data security policies.

347. Defendant further violated the ICFA by failing to notify its clients and former clients of the data breach in a timely manner. The Illinois Personal Information Protection Act requires entities that experience a data breach to notify Illinois residents "in the most expedient time possible and without unreasonable delay." 815 ILCS 530/10.

Violation of the Illinois Personal Information Protection Act constitutes an unlawful practice under the ICFA. 815 ILCS 530/20.

348. Defendant's wrongful practices occurred in the course of trade or commerce.

349. Defendant's wrongful practices were and are injurious to the public interest because those practices were part of a generalized course of conduct on the part of Defendant that applied to all Class members and were repeated continuously before and after Defendant obtained Private Information from Plaintiff and Class members.

350. All Class members have been adversely affected by Defendant conduct and the public was and is at risk as a result thereof.

351. As a direct and proximate result of Defendant's conduct, Plaintiff and Class members have suffered harm, including, but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; and (vii) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains 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 Private Information.

352. Pursuant to 815 ILL. COMP. STAT. § 505/10a(a), Plaintiff seeks actual, compensatory, and punitive damages (pursuant to 815 ILL. COMP. STAT. § 505/10a(c)), injunctive relief, and court costs and attorneys' fees as a result of Defendant's violations of the Illinois CFA.

Count XI – Declaratory Judgment
(By Plaintiffs on behalf of the Class)

353. Plaintiffs restate and reallege all proceeding allegations above and hereafter as if fully set forth herein.

354. Under the Declaratory Judgment Act, 28 U.S.C. § 2201, *et seq.,* this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and to grant further necessary relief. Furthermore, the Court has broad authority to restrain acts that are tortious and violate the terms of the federal and common law described in this Complaint.

355. SLT Lending owes a duty of care to Plaintiffs and Class Members, which required it to adequately secure Plaintiffs' and Class Members' Private Information.

356. SLT Lending still possesses Private Information regarding Plaintiffs and Class Members. 137. Plaintiffs alleges that SLT Lending's data security measures remain inadequate. Furthermore, Plaintiffs continues to suffer injury as a result of the compromise of his Private Information and the risk remains that further compromises of his Private Information will occur in the future.

357. Under its authority pursuant to the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. SLT Lending owes a legal duty to secure its current and former employees' Private Information from unauthorized disclosure and theft;

b. SLT Lending's existing security measures do not comply with its implicit contractual obligations and duties of care to provide reasonable security procedures and practices that are appropriate to protect current and former employees' Private Information; and

c. SLT Lending continues to breach this legal duty by failing to employ reasonable measures to secure current and former employees' Private Information.

358. This Court should also issue corresponding prospective injunctive relief requiring SLT Lending to employ adequate security protocols consistent with legal and industry standards to protect current and former employees' Private Information, including the following:

a. Order SLT Lending to provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members; and

b. Order that, to comply with Defendant's explicit or implicit contractual obligations and duties of care, SLT Lending must implement and maintain reasonable security measures, including, but not limited to:

i. engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on SLT Lending's systems on a periodic basis, and ordering SLT Lending to promptly correct any problems or issues detected by such third-party security auditors;

ii. engaging third-party security auditors and internal personnel to run automated security monitoring;

iii. auditing, testing, and training its security personnel regarding any new or modified procedures;

iv. segmenting its user applications by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of SLT Lending's systems;

v. conducting regular database scanning and security checks;

vi. routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

vii. routinely and continually purging all former employee data that is no longer necessary in order to adequately conduct its business operations; and,

viii. meaningfully educating its users about the threats they face with regard to the security of their Private Information, as well as the steps SLT Lending's current and former employees should take to protect themselves.

359. If an injunction is not issued, Plaintiffs will suffer irreparable injury and will lack an adequate legal remedy to prevent another data breach at SLT Lending. The risk of another such breach is real, immediate, and substantial. If another breach at SLT Lending occurs, Plaintiffs will not have an adequate remedy at law because many of the resulting injuries are not readily quantifiable. 141. The hardship to Plaintiffs if an injunction does not issue exceeds the hardship to SLT Lending if an injunction is issued. Plaintiffs will likely be subjected to substantial, continued identity theft and other related damages if an injunction is not issued. On the other hand, the cost of SLT Lending's compliance with an injunction

requiring reasonable prospective data security measures is relatively minimal, and SLT Lending has a pre-existing legal obligation to employ such measures.

360. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing a subsequent data breach at SLT Lending, thus preventing future injury to Plaintiffs and other current and former employees whose Private Information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE**,** Plaintiffs, on behalf of themselves and Class Members, request judgment against Defendant and that the Court grants the following:

A. For an Order certifying this action as a class action and appointing Plaintiffs and their counsel to represent the Class, California Subclass, and Illinois Subclass, pursuant to Federal Rule of Civil Procedure 23;

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

C. For injunctive relief requested by Plaintiffs, including, but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs 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 their 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 Plaintiffs 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 Plaintiffs and Class Members;

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

v. prohibiting Defendant from maintaining the Private Information of Plaintiffs 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 their security personnel regarding any new or modified procedures; 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;

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

x. 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 Plaintiffs and Class Members;

xi. requiring Defendant to routinely and continually conduct internal training and education, 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;

xii. requiring Defendant to implement a system of tests to assess its respective 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;

xiii. 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;

xiv. requiring Defendant to meaningfully educate The Class about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xv. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and

xvi. 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 actual damages, compensatory damages, statutory damages, and nominal damages, in an amount to be determined, as allowable by law;

E. For an award of punitive damages, as allowable by law;

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

G. Pre- and post-judgment interest on any amounts awarded; and

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

Dated: October 17, 2023

Respectfully submitted,

/s/ Gary M. Klinger

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

Kathleen A. Delaney (#18604-49)
DELANEY & DELANEY LLC
3646 North Washington Blvd.
Indianapolis, IN 46205
Telephone: (317) 920-0400
Email: kathleen@delaneylaw.net

M. Anderson Berry
CLAYEO C. ARNOLD A PROFESSIONAL CORPORATION
865 Howe Avenue
Sacramento, CA 95825
Telephone: (916) 239-4778
Fax: (916) 924-1829
aberry@justice4you.com

SIRI & GLIMSTAD LLP
Mason Barney (pro hac vice to be filed)
Tyler Bean (pro hac vice to be filed)
745 Fifth Avenue, Suite 500
New York, New York 10151
Tel: (212) 532-1091
E: mbarney@sirillp.com
E: tbean@sirillp.com

Counsel for Plaintiffs and the Proposed Class

CERTIFICATE OF SERVICE

The undersigned hereby certifies that on October 17, 2023 the foregoing document was filed via the Court's ECF system, which will cause a true and correct copy of the same to be served electronically on all ECF-registered counsel of record.

/s/ Gary M. Klinger
Gary M. Klinger