





















2021, payment card details for an account balance up to \$1,000 have an average market value of \$150, credit card details with an account balance up to \$5,000 have an average market value of \$240, stolen online banking logins with a minimum of \$100 on the account have an average market value of \$40, and stolen online banking logins with a minimum of \$2,000 on the account have an average market value of \$120.<sup>12</sup>

47. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.<sup>13</sup>

48. Furthermore, trying to change or cancel a stolen Social Security number is no minor task. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

49. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."<sup>14</sup>

---

<sup>12</sup> *Dark Web Price Index 2021*, Zachary Ignoffo, March 8, 2021, available at: <https://www.privacyaffairs.com/dark-web-price-index-2021/> (last accessed December 10, 2021).

<sup>13</sup> Social Security Administration, *Identity Theft and Your Social Security Number*, available at: <https://www.ssa.gov/pubs/EN-05-10064.pdf> (last accessed December 10, 2021).

<sup>14</sup> Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), <http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft> (last accessed December 10, 2021).

50. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, “[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market.”<sup>15</sup>

51. PII can be used to distinguish, identify, or trace an individual’s identity, such as their name and Social Security number. This can be accomplished alone, or in combination with other personal or identifying information that is connected or linked to an individual, such as their birthdate, birthplace, and mother’s maiden name.<sup>16</sup>

52. Given the nature of LLS’s Data Breach, as well as the length of the time LLS’s systems were breached and the long delay in notification to Class Members, it is foreseeable that the compromised PII has been or will be used by hackers and cybercriminals in a variety of devastating ways. Indeed, the cybercriminals who possess Plaintiff’s and Class Members’ PII can easily obtain Plaintiff’s and Class Members’ tax returns or open fraudulent credit card accounts in Class Members’ names.

53. 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 credit card victims can cancel or close credit and debit card accounts.<sup>17</sup> The information compromised in this Data Breach is impossible to “close” and difficult, if not impossible, to change (such as Social Security numbers).

54. To date, LLS has offered its consumers *only two years* of identity monitoring services. The offered services are inadequate to protect Plaintiff and Class Members from the threats they face for years to come, particularly in light of the PII at issue here.

55. The injuries to Plaintiff and Class Members were directly and proximately caused

---

<sup>15</sup> Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, Computer World (Feb. 6, 2015), <http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html> (last accessed December 10, 2021).

<sup>16</sup> See OFFICE OF MGMT. & BUDGET, OMB MEMORANDUM M-07-16 n. 1.

<sup>17</sup> See Jesse Damiani, *Your Social Security Number Costs \$4 On The Dark Web, New Report Finds*, Forbes, Mar 25, 2020, available at: <https://www.forbes.com/sites/jessedamiani/2020/03/25/your-social-security-number-costs-4-on-the-dark-web-new-report-finds/?sh=6a44b6d513f1> (last accessed December 10, 2021).

by LLS's failure to implement or maintain adequate data security measures for its current and former customers.

***Defendant Fails to Comply with FTC Guidelines***

56. 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.

57. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal patient 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.<sup>18</sup> 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.<sup>19</sup>

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

---

<sup>18</sup> 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](https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf) (last visited Mar. 15, 2022).

<sup>19</sup> *Id.*

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

59. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect consumer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act (“FTCA”), 15 U.S.C. § 45.

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

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

62. Defendant was at all times fully aware of its obligation to protect the Personally Identifiable Information of its subjects. Defendant was also aware of the significant repercussions that would result from its failure to do so.

63. Several best practices have been identified that at a minimum should be implemented by companies 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.

64. Other best cybersecurity practices that are standard in the Defendant’s industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such

as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

65. 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.

66. These foregoing frameworks are existing and applicable industry standards in Defendant's industry, and Defendant failed to comply with these accepted standards, thereby opening the door to and causing the Data Breach.

***Defendant's Breach***

67. Defendant breached its obligations to Plaintiff and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data. Defendant's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

- a. Failing to maintain an adequate data security system to reduce the risk of data breaches;
- b. Failing to adequately protect consumers' PII;
- c. Failing to properly monitor its own data security systems for existing intrusions;
- d. Failing to train its employees in the proper handling of data breaches, the protection of PII, and the maintenance of adequate email security practices;
- e. Failing to comply with the FTC guidelines for cybersecurity, in violation of Section 5 of the FTC Act; and,

f. Failing to adhere to industry standards for cybersecurity.

68. Defendant negligently and unlawfully failed to safeguard Plaintiff's and Class Members' PII by allowing cyberthieves to access LLS's IT systems which contained unsecured and unencrypted PII.

69. Accordingly, as outlined below, Plaintiff and Class Members now face an increased risk of fraud and identity theft. In addition, Plaintiff and Class Members also lost the benefit of the bargain they made with Defendant.

### *Harm to Consumers*

70. PII is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

71. There is a strong probability that entire batches of stolen information have been dumped on the black market and are yet to be dumped on the black market, meaning Plaintiff and Class Members are at an increased risk of fraud and identity theft for many years into the future.

72. Thus, Plaintiff and Class Members must vigilantly monitor their financial accounts for many years to come.

73. For example, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines. Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security Numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity. Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security Number 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.

74. Moreover, it is not an easy task to change or cancel a stolen Social Security number.

75. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as “[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number.”<sup>20</sup> The fraudulent activity resulting from the Data Breach may not come to light for years.

76. There may be a time lag between when harm occurs versus when it is discovered, and also between when Personally Identifiable Information is stolen and when it is used.

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

78. Defendant knew or should have known about these dangers and strengthened its data, IT, and email handling systems accordingly. Defendant was put on notice of the substantial and foreseeable risk of harm from a data breach, yet it failed to properly prepare for that risk.

---

<sup>20</sup> Brian Naylor, “*Victims of Social Security Number Theft Find It's Hard to Bounce Back*,” NPR (Feb. 9, 2015), <http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft>.



*Harm to Plaintiff*

79. Prior to the Data Breach, Mr. Guarino provided his PII to LLS for purposes of obtaining a mortgage.

80. In March of 2022, Plaintiff received Notice of Data Breach Letter from LLS informing him that his full name and social security number were stolen by cyberthieves in the Data Breach. As a result of the Data Breach, LLS directed Plaintiff to take certain steps to protect his PII and otherwise mitigate damages.

81. As a result of the Data Breach and the directives that he received in the Notice Letter, Plaintiff spends approximately several hours per week dealing with the consequences of the Data Breach, including, for example, self-monitoring his bank and credit accounts, as well spending time to verify the legitimacy of the *Notice of Data Breach*, communicating with his bank, and exploring credit monitoring and identity theft insurance options. This time has been lost forever and cannot be recaptured.

82. Plaintiff is very careful about sharing his own PII and has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

83. Plaintiff stores any and all documents containing PII in a secure location, and destroys any documents he receives in the mail that contain any PII or that may contain any information that could otherwise be used to compromise her identity and financial accounts. Moreover, he diligently chooses unique usernames and passwords for her various online accounts.

84. Plaintiff suffered actual injury and damages due to LLS's mismanagement of his PII before the Data Breach.

85. Plaintiff suffered actual injury in the form of damages and diminution in the value of his PII—a form of intangible property that he entrusted to LLS for the purpose of providing him mortgage services, which was compromised in and as a result of the Data Breach.

86. Plaintiff suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach, and he has suffered anxiety and increased concerns for the theft of his privacy since he received the Notice Letter. He is especially concerned about the theft of his full name paired with his Social Security number.

87. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his stolen PII, especially his Social Security number, being placed in the hands of unauthorized third-parties and possibly criminals.

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

## **V. CLASS ALLEGATIONS**

89. Plaintiff brings this Action on behalf of herself and on behalf of all other persons similarly situated (the "Class"). Plaintiff proposes the following Class definition, subject to amendment as appropriate:

All persons who utilized LLS's services, whose Personally Identifiable Information was maintained on LLS's system that was compromised in the Data Breach, and who were sent a notice of the Data Breach (the "Class Definition").

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

91. **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 Plaintiff at this time, based on information and belief, the Class consists of over 2,300,000 individuals whose sensitive data was compromised in the Data Breach.

92. **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:

- a. Whether the Defendant unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' Personally Identifiable 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, during, and after the Data Breach complied with the 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, as applicable;
- e. Whether Defendant owed a duty to Class Members to safeguard their Personally Identifiable Information;
- f. Whether Defendant breached a duty to Class Members to safeguard their Personally Identifiable Information;
- g. Whether computer hackers obtained Class Members Personally Identifiable Information in the Data Breach;

- h. Whether the Defendant knew or should have known that its data security systems and monitoring processes were deficient;
  - i. Whether the Plaintiff and Class Members suffered legally cognizable injuries as a result of the Defendant's misconduct;
  - j. Whether Defendant's conduct was negligent;
  - k. Whether Defendant was unjustly enriched by unlawfully retaining a benefit conferred upon them by Plaintiff and Class Members;
  - l. Whether Defendant failed to provide notice of the Data Breach in a timely manner;
  - m. Whether Plaintiff and Class Members are entitled to damages, civil penalties, and/or injunctive relief;
93. **Typicality.** Plaintiff's claims are typical of those of other Class Members because Plaintiff's information, like that of every other Class Member, was compromised in the Data Breach.
94. **Adequacy of Representation.** Plaintiff will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiff's Counsel are competent and experienced in litigating Class actions.
95. **Predominance.** Defendant has engaged in a common course of conduct toward Plaintiff and Class Members, in that all of Plaintiff's and Class Members' data was stored on the same computer system 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.

































