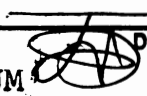


UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF ARKANSAS
CENTRAL DIVISION

FILED
U.S. DISTRICT COURT
EASTERN DISTRICT ARKANSAS

MAY 02 2024

TAMMY H. DOWNS, CLERK
By:  DEP CLERK

KAREN HUGHES, *individually and on behalf of
all others similarly situated,*

Plaintiff,

v.

CENTENNIAL BANK,

Defendant.

Case No.: 4:24-cv-392-JM

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiff Karen Hughes (“Plaintiff”) brings this Class Action Complaint on behalf of herself and all others similarly situated (“Class Members”) against Defendant, Centennial Bank (“Defendant”), alleging as follows based upon information and belief and investigation of counsel, except as to the allegations specifically pertaining to Plaintiff, which are based on personal knowledge:

NATURE OF THE CASE

1. Plaintiff brings this class action against Defendant for its failure to properly secure and safeguard Plaintiff’s and other similarly situated customers’ sensitive personally identifying information (“PII”), including full names, Social Security numbers, dates of birth, driver’s license numbers, bank account numbers, security codes, and health insurance information.

2. Defendant Centennial Bank is a retail bank providing financial services to businesses, investors, and individuals with locations in Arkansas, Florida, Alabama, Texas, and New York.¹

This case assigned to District Judge Moody
and to Magistrate Judge Moore

¹ <https://www.my100bank.com/about-us/>.

3. To obtain banking and other financial services from Defendant, Defendant’s former and current customers were and are required to entrust Defendant with sensitive, non-public PII, without which Defendant could not perform its regular business activities. Defendant retains this information for many years, at least, even after the consumer relationship has ended.

4. Businesses like Defendant that handle PII owe a duty to the individuals to whom that data relates. This duty arises because it is foreseeable that the exposure of PII to unauthorized persons—and especially hackers with nefarious intentions—will result in harm to the affected individuals, including, but not limited to, the invasion of their private financial matters.

5. In or around April 2023, Defendant learned that an unauthorized hacker had gained access to its computer networks. Upon investigating, Defendant confirmed that its network had been penetrated by a cyberattack (the “Data Breach”), through which unauthorized actors accessed and exfiltrated files containing customers’ PII. As a result of its investigation, Defendant concluded on or about March 29, 2024, that Plaintiff’s and Class Members’ PII was compromised in the Data Breach.

6. According to a notice letter Defendant sent to Plaintiff and Class Members on or about April 19, 2024 (the “Notice Letter”), the compromised PII included individuals’ full names, dates of birth, driver’s license numbers, Social Security numbers, bank account numbers and access codes, routing numbers, payment card numbers, and health insurance information.

7. Despite that Defendant became aware of the Data Breach by April 2023, it waited nearly a *full year* before alerting Plaintiff and Class Members that their sensitive PII was exposed.

8. Defendant failed to adequately protect Plaintiff’s and Class Members PII—and failed to even encrypt or redact this highly sensitive information. This unencrypted, unredacted PII was compromised due to Defendant’s intentional, reckless, negligent, and/or careless acts and

omissions and its utter failure to protect customers' sensitive data. Hackers targeted and obtained Plaintiff's and Class Members' PII because of the information's value in exploiting and stealing the identities of Plaintiff and Class Members. The present and continuing risk to victims of the Data Breach will remain for their respective lifetimes.

9. Defendant maintained the PII in a reckless manner. In particular, PII 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 Plaintiff's and Class Members' PII was a known risk to Defendant, and thus, Defendant knew that failing to take reasonable steps to secure the PII left it in a dangerous condition.

10. As a direct and proximate result of Defendant's inadequate data security and breaches of its duties to handle PII with reasonable care, Plaintiff's and Class Members' PII has been accessed by hackers and exposed to an untold number of unauthorized individuals.

11. The harm resulting from a data breach manifests in numerous ways including identity theft and financial fraud, and the exposure of an individual's PII due to a data breach ensures that the individual will be at a substantially increased and certainly impending risk of identity theft crimes compared to the rest of the population, potentially for the rest of his or her life. Mitigating that risk, to the extent it is even possible to do so, requires individuals to devote significant time and money to closely monitor their credit, financial accounts, and email accounts, and take several additional prophylactic measures.

12. As a result of Defendant's conduct and the resulting Data Breach, Plaintiff and Class Members suffered concrete injuries in fact including, but not limited to (a) invasion of privacy; (b) financial costs incurred mitigating the materialized risk and imminent threat of identity theft; (c) loss of time and loss of productivity incurred mitigating the materialized risk and

imminent threat of identity theft; (d) financial costs incurred due to actual identity theft; (e) loss of time incurred due to actual identity theft; (f) deprivation of value of their PII; and (g) the continued risk to their sensitive PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII it collects and maintains.

13. To recover from Defendant for these harms, Plaintiff, on behalf of herself and the Class as defined herein, brings claims for negligence, breach of implied contract, breach of fiduciary duty, breach of confidence, and unjust enrichment to address Defendant's inadequate safeguarding of Plaintiff's and Class Members' PII it collected and maintained, and for failing to provide timely and adequate notice to Plaintiff and other Class Members that their information had been subject to the unauthorized access by an unknown party in the Data Breach.

14. Plaintiff and Class Members seek damages in an amount to be determined at trial, declaratory judgment, and injunctive relief requiring Defendant to (a) disclose, expeditiously, the full nature of the Data Breach and the types of PII accessed, obtained, or exposed by the hackers; (b) implement improved data security practices to reasonably guard against future breaches of PII possessed by Defendant; and (c) provide, at Defendant's own expense, all impacted victims with lifetime identity theft protection services.

PARTIES

15. Plaintiff Karen Hughes is an adult individual who at all relevant times has been a citizen and resident citizen of White Deer, Texas.

16. Plaintiff was a Centennial Bank customer and account holder.

17. In the course of receiving services from Defendant, Plaintiff was required to supply Defendant with her PII—including, but not limited to her full name, date of birth, Social Security

number, driver's license number, account number and access code, payment card number, and health insurance information.

18. Plaintiff greatly values her privacy and diligently protects her PII.

19. Plaintiff would not have provided her PII to Defendant if she had known that her PII would be maintained using inadequate data security systems.

20. On or about April 19, 2024, Plaintiff received the Notice Letter from Defendant advising her of the Data Breach. According to the Notice Letter, unauthorized, unknown actors gained access to Defendant's computer network on or about April 6 and 7, 2023, and accessed and acquired files containing Plaintiff's sensitive PII, including her full name, date of birth, driver's license number, Social Security number, bank account number and access code, routing number, payment card number, and health insurance information.

21. In response to the Data Breach and the Notice Letter, Plaintiff has made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach and reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud. Plaintiff monitors her financial and credit statements multiple times a week and has already spent many hours dealing with the Data Breach, valuable time Plaintiff otherwise would have spent on other activities.

22. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. Due to the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

23. The risk of identity theft is not speculative or hypothetical, but is impending and has materialized, as there is evidence that Plaintiff and Class Members' PII was targeted, accessed,

misused, and disseminated on the Dark Web.

24. Other than the Data Breach, Plaintiff is not aware of ever being part of a data breach or similar cybersecurity incident involving her PII and is concerned that it has now been exposed to bad actors.

25. Subsequent to the Data Breach, Plaintiff has suffered numerous, substantial injuries including, but not limited to: (a) financial costs incurred mitigating the materialized risk and imminent threat of identity theft; (b) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft; (c) financial costs incurred due to actual identity theft; (d) loss of time incurred due to actual identity theft; (e) deprivation of value of their PII; (f) invasion of privacy; and (g) the continued risk to her sensitive PII, which remains in the possession of Defendant, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect the PII it collects and maintains.

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

27. Plaintiff has a continuing interest in ensuring that her PII, which, upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches.

28. Defendant Centennial Bank is an Arkansas-based corporation with its principal place of business located at 620 Chestnut Street, Conway, Arkansas 72033.

JURISDICTION AND VENUE

29. This Court has original jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2), because this is a class action in which at least one member of the putative Class, as defined below, are citizens of a different state than Defendant, there are more

than 100 putative class members, and the amount in controversy exceeds \$5 million exclusive of interest and costs.

30. This Court has general personal jurisdiction over Defendant because Defendant maintains its principal place of business is in Arkansas and regularly conducts business in Arkansas giving rise to sufficient minimum contacts with this state, and because the acts and omissions giving rise to Plaintiff's claims occurred in and emanated from this state.

31. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)(1) because Defendant's principal place of business is in this District and a substantial part of the events, acts, and omissions giving rise to Plaintiff's claims occurred in this District.

FACTUAL BACKGROUND

A. Defendant Knew the Risks of Storing Valuable PII and the Foreseeable Harm to Victims.

32. Defendant provides retail banking services services to customers around the country, including in Arkansas, Florida, Alabama, Texas, and New York.

33. Plaintiff and Class Members are current and former customers of Defendant.

34. As a condition of receiving its banking services, Defendant requires that its customers, including Plaintiff and Class Members, entrust Defendant with highly sensitive PII.

35. The information Defendant held in its systems or those of at the time of the Data Breach included the unencrypted PII of Plaintiff and Class Members.

36. At all relevant times, Defendant knew it was storing and using its system and networks to transmit valuable, sensitive PII, and that as a result, Defendant's systems would be attractive targets for cybercriminals.

37. Defendant also knew that any breach of its computer systems and exposure of the information stored therein would result in the increased risk of identity theft and fraud against the

individuals whose PII was compromised, as well as intrusion into those individuals' highly private financial information.

38. Upon information and belief, Defendant made promises and representations to its customers, including Plaintiff and Class Members, that the PII collected from them as a condition of obtaining products and/or services from Defendant would be kept safe, confidential, that the privacy of that information would be maintained, and that Defendant would delete any sensitive information after it was no longer required to maintain it.

39. Indeed, Defendant's Privacy Policy warrants: "To protect your personal information from unauthorized access and use, we use security measures that comply with federal law. These measures include computer safeguards and secured files and buildings."²

40. Plaintiff and the Class Members, as former and current customers of Defendant, relied on these promises from this sophisticated business entity to keep their sensitive PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. Consumers, in general, demand security to safeguard their PII, especially when Social Security numbers and other sensitive financial is involved.

41. Based on the foregoing representations and warranties and in order to obtain Defendant's products and/or services, Plaintiff and Class Members provided at least the following PII to Defendant with the reasonable expectation and on the mutual understanding that Defendant would comply with its promises and obligations to keep such information confidential and secure from unauthorized access:

² https://www.my100bank.com/privacy-policy/?_gl=1%2Auah16r%2A_ga%2AMjc2NjMyMTQ5LjE3MTQ1Njk5NzE.%2A_ga_6KVF9NWEWW%2AMTcxNDU2OTk3MC4xLjEuMTcxNDU3MTE1OS41Mi4wLjA.

- a. names;
- b. addresses;
- c. dates of birth;
- d. Social Security numbers;
- e. driver's license numbers;
- f. bank/financial account and routing numbers and access codes;
- g. payment card information; and
- h. health insurance information.

42. Plaintiff and Class Members value the confidentiality of their PII and demand security to safeguard their PII. To that end, Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII.

43. Plaintiff and Class Members relied on the sophistication of Defendant to keep their PII confidential and securely maintained, to use this information for necessary purposes only and make only authorized disclosures of this information, and to delete PII from Defendant's systems when no longer necessary for its legitimate business purposes.

44. Defendant had and has the duty to adopt reasonable measures to protect Plaintiff's and Class Members' PII from involuntary disclosure to third parties and to audit, monitor, and verify the integrity of data management systems and those of its vendors and affiliates. Defendant had and has the legal duty to keep customers' and consumers' PII safe and confidential.

45. Defendant had and has obligations created by the Federal Trade Commission Act, 15 U.S.C. § 45 ("FTC Act"), Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801-6809, §§ 6821-6827 ("GLBA"), contract, industry standards, and representations made to Plaintiff and Class Members, to keep their PII confidential and to protect it from unauthorized access and disclosure.

46. Defendant derived a substantial economic benefit from collecting Plaintiff's and Class Members' PII. Without the required submission of PII, Defendant could not perform the services it provides.

47. By obtaining, using, and benefitting from Plaintiff's and Class Members' PII, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' PII from unauthorized disclosure.

B. The Data Breach

48. On or about April 19, 2024, Defendant began sending Plaintiff and other Data Breach victims Notice Letters informing that “[i]n April 2023, someone temporarily accessed Centennial’s computer network without permission” and copied files containing customers’ sensitive PII.

49. According to the Notice Letter, on or about March 29, 2024, Defendant determined that the files exposed through the Data Breach included the following PII:

- Customer name
- Social Security number
- Driver’s license number
- Bank name
- Bank account number
- Bank routing number
- Payment card number
- Account PIN/security code/access code
- Financial account type
- Medicare/Medicaid identification

- Health insurance subscriber number

50. Omitted from the Notice Letter were the details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure such a breach does not occur again. To date, these critical facts have not been explained or clarified to Plaintiff and Class Members, who retain a vested interest in ensuring that their PII remains protected.

51. Defendant's "disclosure" amounts to no real disclosure at all, as it fails to inform Plaintiff and Class Members of the Data Breach's critical facts with any degree of specificity. Without these details, Plaintiff's and Class Members' ability to mitigate the harms resulting from the Data Breach is severely diminished.

52. Based on Defendant's statements, it is evident that the bad actors accessed its computer systems in an intentional attack designed to acquire customers' valuable PII stored therein, and that the bad actors were successful in the attack.

53. Plaintiff's and Class Members' PII was accessed and stolen in the Data Breach and is now in the hands of cybercriminals.

54. The hacker accessed and acquired files Defendant stored on its systems, which contained unencrypted PII of Plaintiff and Class Members.

55. Plaintiff further believes her PII, and that of Class Members, was subsequently sold on the dark web following the Data Breach, as that is the modus operandi of cybercriminals that commit cyber-attacks of this type. Moreover, following the Data Breach, Plaintiff has experienced suspicious spam and believes this be an attempt to secure additional PII from her.

56. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive PII it was collecting and maintaining from Plaintiff and Class Members, such as encrypting the information or deleting it when it is no longer needed, which caused the

exposure of PII. Moreover, Defendant failed to promptly notify Plaintiff and Class Members upon discovering the Data Breach, waiting nearly *one full year* to send Notice Letters after the Data Breach occurred.

57. Defendant could have prevented this Data Breach by properly securing and encrypting the files containing Plaintiff's and Class Members' PII.

58. Upon information and belief, Defendant made promises to Plaintiff and Class Members to maintain and protect their PII, demonstrating an understanding of the importance of securing PII.

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

C. Defendant Knew or Should Have Known that Companies in Possession of PII Are Particularly Susceptible to Cyber Attacks and at Risk for a Data Breach.

60. At all relevant times, Defendant knew it was storing and permitting its employees to use its computer networks to store valuable, sensitive PII and that, as a result, Defendant's systems would be attractive targets for cybercriminals.

61. Defendant also knew that any breach of its systems, and exposure of the information stored therein would result in the increased risk of identity theft and fraud against the individuals whose PII was compromised, as well as intrusion into their highly private financial information.

62. These risks are not merely theoretical; in recent years, numerous high-profile breaches have occurred at businesses such as CapitalOne, KeyBank, Equifax, Flagstar Bank, and TMX Finance Corporate Services, and many others.

63. PII has considerable value and constitutes an enticing and well-known target to hackers. Hackers easily can sell stolen data as a result of the "proliferation of open and anonymous

cybercrime forums on the Dark Web that serve as a bustling marketplace for such commerce.”³

64. As the Federal Trade Commission (“FTC”) recognizes, identity thieves can use PII to commit an array of crimes including identity theft, and medical and financial fraud.⁴ Indeed, a robust “cyber black market” exists in which criminals openly post stolen PII and other protected financial information on multiple underground Internet websites, commonly referred to as the “dark web.”

65. Criminals often trade stolen PII on the “cyber black market” for years following a breach. Cybercriminals can also post stolen PII on the internet, thereby making such information publicly available.

66. The prevalence of data breaches and identity theft has increased dramatically in recent years, accompanied by a parallel and growing economic drain on individuals, businesses, and government entities in the United States. In 2021, there were 4,145 publicly disclosed data breaches, exposing 22 billion records. The United States specifically saw a 10% increase in the total number of data breaches.⁵

67. In tandem with the increase in data breaches, the rate of identity theft and the resulting losses has also increased over the past few years. For instance, in 2018, 14.4 million people were victims of some form of identity fraud, and 3.3 million people suffered unrecouped

³ Brian Krebs, *The Value of a Hacked Company*, Krebs on Security (July 14, 2016), <http://krebsonsecurity.com/2016/07/the-value-of-a-hacked-company/>.

⁴ *What To Know About Identity Theft*, FED. TRADE COMM’N CONSUMER ADVICE (Apr. 2021), <https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft> (last accessed Jan 23, 2024).

⁵ *Data Breach Report: 2021 Year End*, RISK BASED SECURITY (Feb. 4, 2022), <https://www.riskbasedsecurity.com/2022/02/04/data-breach-report-2021-year-end/>.

losses from identity theft, nearly three times as many as in 2016. And these out-of-pocket losses more than doubled from 2016 to \$1.7 billion in 2018.⁶

68. The financial sector is also a prime target for threat actors. Between January 2018 and September 2023, financial companies have suffered 2,260 data breaches, impacting over 232 million records.⁷

69. The financial sector is “disproportionately targeted by threat actors” because of a simple rationale: “[t]hreat actors target organizations that have what they want and what pays big – data and money. Data can be sold for money and vulnerabilities that enable access to both data and money.”⁸

70. Indeed, “[h]acking financial organizations can potentially allow malicious threat actors to access accounts or personal information that can help a criminal gain unauthorized access and make financial transactions or trick others into revealing more information and sending them money.”⁹

71. According to the United States Government Accountability Office, which conducted a study regarding data breaches, “in some cases, stolen data may be held for up to a

⁶ Insurance Information Institute, *Facts + Statistics: Identity theft and cybercrime*, available at [https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime#Identity%20Theft%20And%20Fraud%20Reports,%202015-2019%20\(1\)](https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime#Identity%20Theft%20And%20Fraud%20Reports,%202015-2019%20(1)).

⁷ Paul Bischoff, *Financial data breaches accounted for 232 million leaked records from January 2018 to September 2023*, Comparitech (Oct. 4, 2023), <https://www.comparitech.com/blog/vpn-privacy/financial-data-breaches/#:~:text=2%2C260%20financial%20data%20breaches%20from,over%20101%20million%20in%20total>.

⁸ Jen Miller-Osborn, *3 Reasons Cyberattacks Target Financial Services and How to Fight Back*, Paloalto Network (Aug. 31, 2021), <https://www.paloaltonetworks.com/blog/2021/08/financial-services-cyberattacks/>.

⁹ Kyle Chin, *Why is the Finance Sector a Target for Cyber Attacks?*, UpGuard (Aug. 21, 2023), <https://www.upguard.com/blog/finance-sector-cyber-attacks/#:~:text=Hacking%20financial%20organizations%20can%20potentially,information%20and%20sending%20them%20money>.

year or more before being used to commit identity theft. Further, once stolen data has been sold or posted on the [Dark] 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.”¹⁰

72. The breadth of data compromised in the Data Breach makes the information particularly valuable to thieves and leaves Plaintiff and Class Members especially vulnerable to identity theft, tax fraud, credit and bank fraud, and more.

73. **Social Security Numbers**—Unlike credit or debit card numbers in a payment card data breach—which can quickly be frozen and reissued in the aftermath of a breach—unique social security numbers cannot be easily replaced. Even when such numbers are replaced, the process of doing so results in a major inconvenience to the subject person, requiring a wholesale review of the person’s relationships with government agencies and any number of private companies in order to update the person’s accounts with those entities.

74. The Social Security Administration even warns that the process of replacing a Social Security number is a difficult one that creates other types of problems, and that it will not be a panacea for the affected person:

Keep in mind that a new number probably will not solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) likely will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So using a new number will not guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same.

If you receive a new Social Security Number, you should not be able to use the old number anymore.

¹⁰ United States Government Accountability Office, Report to Congressional Requesters, Personal Information, June 2007: <https://www.gao.gov/assets/gao-07-737.pdf>.

For some victims of identity theft, a new number actually creates new problems. If the old credit information is not associated with your new number, the absence of any credit history under the new number may make more difficult for you to get credit.^[11]

75. Social Security Numbers allow individuals to apply for credit cards, student loans, mortgages, and other lines of credit—among other services. Often social security numbers can be used to obtain medical goods or services, including prescriptions. They are also used to apply for a host of government benefits. Access to such a wide range of assets makes social security numbers a prime target for cybercriminals and a particularly attractive form of PII to steal and then sell.

76. A data breach increases the risk of becoming a victim of identity theft. Victims of identity theft can suffer from both direct and indirect financial losses. According to a research study published by the Department of Justice:

A direct financial loss is the monetary amount the offender obtained from misusing the victim's account or personal information, including the estimated value of goods, services, or cash obtained. It includes both out-of-pocket loss and any losses that were reimbursed to the victim. An indirect loss includes any other monetary cost caused by the identity theft, such as legal fees, bounced checks, and other miscellaneous expenses that are not reimbursed (e.g., postage, phone calls, or notary fees). All indirect losses are included in the calculation of out-of-pocket loss.^[12]

77. Even if stolen PII does not include financial or payment card account information, that does not mean there has been no harm, or that the breach does not cause a substantial risk of identity theft. Freshly stolen information can be used with success against victims in specifically targeted efforts to commit identity theft known as social engineering or spear phishing. In these

¹¹ Social Security Administration, *Identity Theft and Your Social Security Number*, July 2021, available at <https://www.ssa.gov/pubs/EN-05-10064.pdf> (last accessed April 30, 2024).

¹² Erika Harrell, *Bureau of Just. Stat.*, U.S. DEP'T OF JUST., NCJ 256085, *Victims of Identity Theft*, 2018 I (2020) <https://bjs.ojp.gov/content/pub/pdf/vit18.pdf> (last accessed Jan. 23, 2024).

forms of attack, the criminal uses the previously obtained PII about the individual, such as name, address, email address, and affiliations, to gain trust and increase the likelihood that a victim will be deceived into providing the criminal with additional information.

78. A poll of security executives predicted an increase in attacks over the next two years from “social engineering and ransomware” as nation-states and cybercriminals grow more sophisticated. Unfortunately, these preventable causes will largely come from “misconfigurations, human error, poor maintenance, and unknown assets.”¹³

79. Due to high-profile data breaches at other financial institutions, Defendant knew or should have known that its information technology system would be targeted by cybercriminals.

80. Defendant also knew or should have known the importance of safeguarding the PII with which it was entrusted and of the foreseeable consequences if its data security systems were breached. Defendant failed, however, to take adequate cybersecurity measures to prevent the Data Breach and the exfiltration of its customers’ PII from occurring.

81. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant’s server(s), namely, the detailed, sensitive PII of tens of thousands of individuals, if not more, and thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

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

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

¹³ Chuck Brooks, *Alarming Cyber Statistics For Mid-Year 2022 That You Need to Know*, FORBES (June 3, 2022), <https://www.forbes.com/sites/chuckbrooks/2022/06/03/alarming-cyber-statistics-for-mid-year-2022-that-you-need-to-know/?sh=176bb6887864>.

by Defendant's failure to implement or maintain adequate data security measures for Plaintiff's and Class Members' PII.

D. Value Of Personally Identifiable Information

84. The 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 "[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

85. 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

86. For example, PII can be sold at a price ranging from \$40 to \$200.¹⁷ Criminals can also purchase access to entire company data breaches from \$900 to \$4,500.¹⁸

87. 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

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, <https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/> (last visited Feb. 26, 2024).

¹⁷ *Here's How Much Your Personal Information Is Selling for on the Dark Web*, EXPERIAN, Dec. 6, 2017, <https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/> (last visited Feb. 26, 2024).

¹⁸ *In the Dark*, VPNOVERVIEW, 2019, <https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/> (last visited Feb. 26, 2024).

compromised in this Data Breach is impossible to “close” and difficult, if not impossible, to change—names, dates of birth, contact information, and medical device information.

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.”¹⁹

E. Defendant Failed to Comply with FTC Guidelines and Industry Best Practices.

88. Defendant is prohibited by the FTC Act from engaging in “unfair or deceptive acts or practices in or affecting commerce.” The FTC has concluded that a company’s failure to maintain reasonable and appropriate data security for consumers’ sensitive personal information is an “unfair practice” in violation of the FTC Act.

89. The FTC has promulgated numerous guides for businesses that 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.²⁰

90. The FTC recommends the following practices:

- a. Identify all connections to the computers where sensitive information is stored;
- b. Assess the vulnerability of each connection to commonly known or reasonably foreseeable attacks;
- c. Do not store sensitive consumer data on any computer with an internet connection unless it is essential for conducting their business;
- d. Scan computers on their network to identify and profile the operating system and open network services. If services are not needed, they should be disabled to prevent hacks or other potential security problems. For example, if email

¹⁹ Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT WORLD (Feb. 6, 2015), <https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html> (last visited Feb. 26, 2024).

²⁰ *Start with Security: A Guide for Business*, U.S. Federal Trade Comm’n (2015), <https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf>.

service or an internet connection is not necessary on a certain computer, a business should consider closing the ports to those services on that computer to prevent unauthorized access to that machine;

- e. Pay particular attention to the security of their web applications—the software used to give information to visitors to their websites and to retrieve information from them. Web applications may be particularly vulnerable to a variety of hack attacks;
- f. Use a firewall to protect their computers from hacker attacks while it is connected to a network, especially the internet;
- g. Determine whether a border firewall should be installed where the business’s network connects to the internet. A border firewall separates the network from the internet and may prevent an attacker from gaining access to a computer on the network where sensitive information is stored. Set access controls—settings that determine which devices and traffic get through the firewall—to allow only trusted devices with a legitimate business need to access the network. Since the protection a firewall provides is only as effective as its access controls, they should be reviewed periodically;
- h. Monitor incoming traffic for signs that someone is trying to hack in. Keep an eye out for activity from new users, multiple log-in attempts from unknown users or computers, and higher-than average traffic at unusual times of the day; and
- i. Monitor outgoing traffic for signs of a data breach. Watch for unexpectedly large amounts of data being transmitted from their system to an unknown user. If large amounts of information are being transmitted from a business’s network, the transmission should be investigated to make sure it is authorized.^[21]

91. The FTC further recommends business take additional cybersecurity steps, which include the following:

- a. Conducting an inventory of all company devices that store sensitive data, and understanding what types of PII is stored on those devices;
- b. Encrypting sensitive personal information stored on computer networks so that it is unreadable even if hackers are able to gain access to the information;

²¹ *Protecting Personal Information: A Guide for Business*, U.S. Federal Trade Comm’n (2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

- c. Crafting a data security plan that involves both physical security (*e.g.*, locking up physical files) and electronic security, and training employees regarding the data security plan.
- d. Promptly disposing of PII that is no longer needed, and retaining sensitive data only as long as companies maintain a legitimate business need for the information; and
- e. Developing a plan to handle a data breach or data security incident, if and when such an incident occurs.^[22]

92. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

93. Upon information and belief, Defendant failed to properly implement one or more of the basic data security practices described above. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to consumer PII resulted in the unauthorized access to and exfiltration of Plaintiff's and Class Members' PII.

94. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data constitutes an unfair act of practice prohibited by Section 5 of the FTC Act.

95. Similarly, the U.S. Government's National Institute of Standards and Technology ("NIST") provides a comprehensive cybersecurity framework that companies of any size can use to evaluate and improve their information security controls.²³

²² *Id.*

²³ See Framework for Improving Critical Infrastructure Cybersecurity, NAT'L INST. OF STANDARDS & TECH. (April 16, 2018), Appendix A, Table 2, <https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf>.

96. NIST publications include substantive recommendations and procedural guidance pertaining to a broad set of cybersecurity topics including risk assessments, risk management strategies, access controls, training, data security controls, network monitoring, breach detection, and incident response. Upon information and belief, Defendant failed to adhere to the NIST guidance.

97. Further, cybersecurity experts have identified various best practices that should be implemented by entities in the financial industry, including the following:²⁴

- a. Regularly assessing risks and auditing cybersecurity;
- b. Establishing a cybersecurity policy;
- c. Appointing a data protection officer;
- d. Securing networks;
- e. Verifying user identities;
- f. Establishing secure password management;
- g. Continuously monitor user activity; and
- h. Manage third-party risks.

98. Upon information and belief, Defendant's failure to protect Plaintiff's and Class Members' PII is a result of its failure to adopt reasonable safeguards as required by the FTC, NIST, and industry best practices.

99. Defendant was, at all times, fully aware of its obligations to protect the PII of consumers because of its business model of collecting PII to provide financial services. Defendant was also aware of the significant repercussions that would result from its failure to do so.

²⁴ *12 Best Practices for Banking and Financial Cybersecurity Compliance*, Ekran (July 17, 2023), <https://www.ekransystem.com/en/blog/banking-and-financial-cyber-security-compliance>.

F. Defendant is Subject to, and Failed to Comply with, the GLBA.

100. The GLBA states, “It is the policy of the Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers’ nonpublic personal information.” 15 U.S.C. § 6801(a).

101. A “financial institution” is defined as “any institution the business of which is engaging in financial activities as described in section 1843(k) of title 12.” 15 U.S.C. § 6809(3)(A). Defendant is considered a financial institution for purposes of the GLBA as Defendant offers consumers financial products and/or services. *See* 12 U.S.C. § 1843(k)(4).

102. “Nonpublic personal information” means “personally identifiable financial information provided by a consumer to a financial institution; resulting from any transaction with the consumer or any service performed for the consumer; or otherwise obtained by the financial institution.” 15 U.S.C. § 6809(4)(A)(i)–(iii).

103. The PII involved in the Data Breach constitutes “nonpublic personal information” for purposes of the GLBA.

104. Defendant collects “nonpublic personal information,” as defined by 15 U.S.C. § 6809(4)(A), 16 C.F.R. § 313.3(n) & 12 C.F.R. § 1016.3(p)(1). Accordingly, during the relevant time period, Defendant was subject to the requirements of the GLBA, 15 U.S.C. §§ 6801, et seq., and to numerous rules and regulations promulgated under the GLBA.

105. The Safeguards Rule, which implements Section 501(b) of the GLBA, 15 U.S.C. § 6801(b), requires financial institutions to protect the security, confidentiality, and integrity of customer information by developing a comprehensive written information security program that contains reasonable administrative, technical, and physical safeguards, including: (1) designating

one or more employees to coordinate the information security program; (2) identifying reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information, and assessing the sufficiency of any safeguards in place to control those risks; (3) designing and implementing information safeguards to control the risks identified through risk assessment, and regularly testing or otherwise monitoring the effectiveness of the safeguards' key controls, systems, and procedures; (4) overseeing service providers and requiring them by contract to protect the security and confidentiality of customer information; and (5) evaluating and adjusting the information security program in light of the results of testing and monitoring, changes to the business operation, and other relevant circumstances. 16 C.F.R. §§ 314.3 & 314.4. As alleged herein, Defendant violated the Safeguards Rule.

106. Defendant's conduct resulted in a variety of failures to follow GLBA-mandated rules and regulations, many of which are also industry standard. Among such deficient practices, the Data Breach demonstrates that Defendant failed to implement (or inadequately implemented) information security policies or procedures such as effective employee training, adequate intrusion detection systems, regular reviews of audit logs and records, and other similar measures to protect the confidentiality of the PII it maintained in its information technology systems.

107. Had Defendant implemented data security protocols, the consequences of the Data Breach could have been avoided, or at least significantly reduced as the Data Breach could have been detected earlier, the amount of PII compromised could have been greatly reduced.

G. Defendant Breached its Duties to Safeguard Plaintiff's and Class Members' PII.

108. In addition to its obligations under federal and state laws, Defendant owed a duty to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII in its possession from being compromised, lost,

stolen, accessed, and misused by unauthorized persons. Defendant owed a duty to Plaintiff and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its servers, computer systems, networks, and protocols adequately protected Plaintiff's and Class Members' PII.

109. Defendant breached its obligations to Plaintiff and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard their servers, 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 that would reduce the risk of data breaches and cyberattacks;
- b. Failing to adequately protect customers' PII;
- c. Failing to properly monitor its data security systems for existing intrusions;
- d. Failing to sufficiently train its employees and vendors regarding the proper handling of customers' PII;
- e. Failing to fully comply with FTC guidelines for cybersecurity in violation of the FTCA and GLBA; and
- f. Otherwise breaching its duties and obligations to protect Plaintiff's and Class Members' PII.

110. Defendant negligently and unlawfully failed to safeguard Plaintiff's and Class Members' PII by allowing cyberthieves to access Defendant's servers and data management systems which contained unsecured and unencrypted PII.

111. Had Defendant remedied the deficiencies in its information storage and security systems, followed industry guidelines, and adopted security measures recommended by experts in the field, it could and would have prevented intrusion into their information storage and security systems and, ultimately, the theft of Plaintiff's and Class Members' confidential PII.

H. Common Injuries & Damages

112. As a result of Defendant's ineffective and inadequate data security practices, the Data Breach, and the foreseeable consequences of PII ending up in the possession of criminals, the risk of identity theft to Plaintiff and Class Members has materialized and is imminent, and Plaintiff and Class Members have all sustained actual injuries and damages, including, without limitation, (a) invasion of privacy; (b) financial costs incurred mitigating the materialized risk and imminent threat of identity theft; (c) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft; (d) financial costs incurred due to actual identity theft; (e) loss of time incurred due to actual identity theft; (f) deprivation of value of their PII; and (g) the continued risk to their sensitive PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII it collects and maintains.

I. The Data Breach Increases Victims' Risk of Identity Theft.

113. Plaintiff and the Class Members are at a heightened risk of identity theft for years to come.

114. The unencrypted PII of Plaintiff and Class Members will end up for sale on the dark web because that is the *modus operandi* of hackers. In addition, unencrypted PII may fall into the hands of companies that will use the detailed PII for targeted marketing without the approval of Plaintiff and Class Members. Unauthorized individuals can easily access the Plaintiff's and Class Members' PII.

115. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal PII to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the

information to commit a variety of identity theft related crimes discussed below.

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

117. 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 victim.

118. One such example of criminals piecing together bits and pieces of compromised PII for profit is the development of “Fullz” packages.²⁵

119. With “Fullz” packages, cyber-criminals can cross-reference two sources of PII to

²⁵ “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 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://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-firm> (last visited Feb. 26, 2024).

marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy to assemble complete dossiers on individuals.

120. The development of “Fullz” packages means here that the stolen PII from the Data Breach can easily be used to link and identify it to Plaintiff’s 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 PII 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.

121. The existence and prevalence of “Fullz” packages means that the PII stolen from the Data Breach can easily be linked to the unregulated data (like driver's license numbers) of Plaintiff and the other Class Members.

122. Thus, even if certain information (such as driver's license numbers) was not stolen in the data breach, criminals can still easily create a comprehensive “Fullz” package.

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

J. Loss Of Time to Mitigate Risk of Identity Theft and Fraud

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

125. Thus, due to the actual and imminent risk of identity theft, Plaintiff and Class Members must monitor their financial accounts for many years to mitigate that risk.

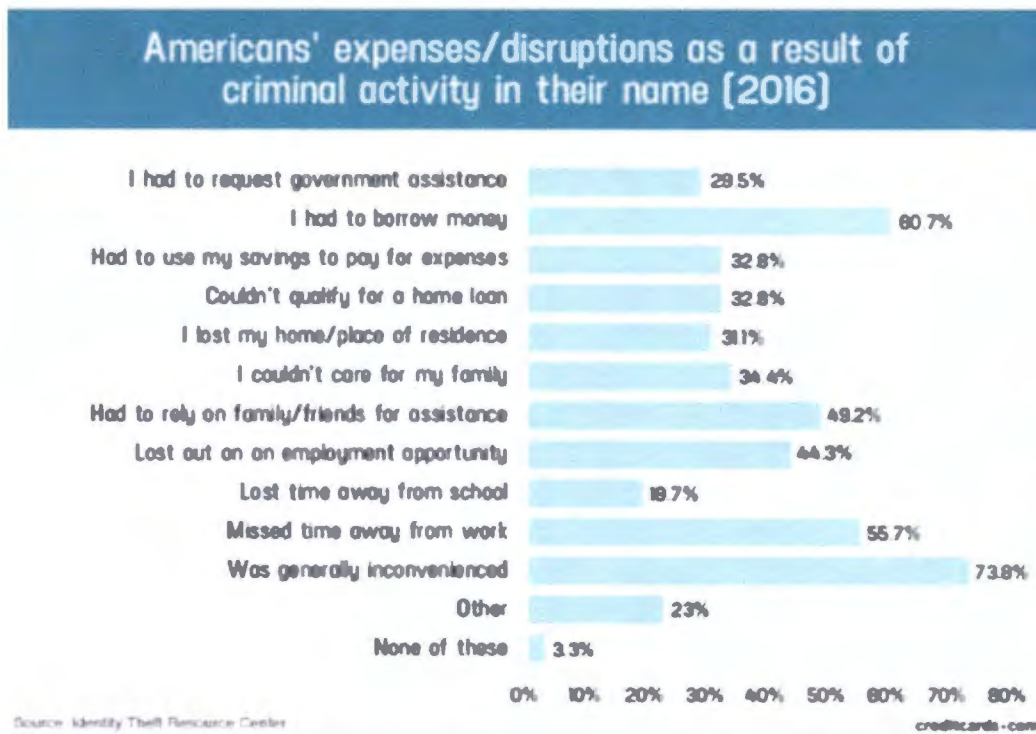
126. Plaintiff and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions to remedy the harms they have or may experience as a result of the Data Breach, such as contacting credit bureaus to place freezes on their accounts; changing passwords and resecuring their own computer networks; and checking their financial accounts for any indication of fraudulent activity, which may take years to detect.

127. These efforts are consistent with the steps that FTC recommends that data breach victims take several steps to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.²⁶

128. A study by Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:²⁷

²⁶ See Federal Trade Commission, *Identity Theft.gov*, <https://www.identitytheft.gov/Steps> (last visited Feb. 26, 2024).

²⁷ Jason Steele, “Credit Card and ID Theft Statistics,” Oct. 24, 2017, <https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php> (last visited Feb. 26, 2024).



129. And for those Class Members who experience actual identity theft and fraud, the GAO released a report in 2007 regarding data breaches, 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

K. Diminution Value Of PII

130. PII is a valuable property right.²⁹ Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that PII has

²⁸ See “Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown,” at 2, U.S. GOV’T ACCOUNTABILITY OFFICE, June 2007, <https://www.gao.gov/new.items/d07737.pdf> (last visited Feb. 26, 2024) (“GAO Report”).

²⁹ See, e.g., Randall T. Soma, et al., Corporate Privacy Trend: The “Value” of Personally Identifiable Information (“PII”) Equals the “Value” of Financial Assets, 15 RICH. J.L. & TECH. 11, at *3-4 (2009) (“PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.”) (citations omitted).

considerable market value.

131. An active and robust legitimate marketplace for PII exists. In 2019, the data brokering industry was worth roughly \$200 billion.³⁰

132. 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.^{31,32}

133. Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to \$50.00 a year.³³ Conversely, sensitive PII can sell for as much as \$363 per record on the dark web according to the Infosec Institute.³⁴

134. 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, e.g., name, contact information, dates of birth, medical device information.

135. As a result of the Data Breach, Plaintiff’s and Class Members’ PII, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its compromise and unauthorized release. However, this transfer of value occurred without any consideration paid to Plaintiff or Class Members for their property, resulting in an economic loss.

³⁰ <https://www.latimes.com/business/story/2019-11-05/column-data-brokers> (last visited Feb. 26, 2024).

³¹ <https://datacoup.com/> (last visited Feb. 26, 2024).

³² <https://digi.me/what-is-digime/> (last visited Feb. 26, 2024).

³³ Nielsen Computer & Mobile Panel, *Frequently Asked Questions*, <https://computermobilepanel.nielsen.com/ui/US/en/faqs.html> (last visited Feb. 26, 2024).

³⁴ 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 Feb. 26, 2024).

Moreover, the PII is now readily available, and the rarity of the Data has been lost, thereby causing additional loss of value.

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

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

137. Given the type of targeted attack in this case and sophisticated criminal activity, the type of PII involved, and the volume of data obtained in the Data Breach, there is a strong probability that entire batches of stolen information have been or will be placed on the black market/dark web for sale and purchase by criminals intending to utilize the PII for identity theft crimes—*e.g.*, opening bank accounts in the victims' names to make purchases or launder money; filing false tax returns; taking out loans or lines of credit; or filing false unemployment claims.

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

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

140. The retail cost of credit monitoring and identity theft monitoring can cost around \$200 a year per Class Member. This is reasonable and necessary cost to monitor to protect Plaintiff and Class Members from the risk of identity theft that arose from the Data Breach caused by Defendant's deficient data security processes. This is a future cost for a minimum of five years

that Plaintiff and Class Members would not need to bear but for Defendant's failure to safeguard their PII.

M. Loss of the Benefit of the Bargain

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

CLASS ACTION ALLEGATIONS

142. Plaintiff brings this action individually and on behalf of all other persons similarly situated, pursuant to Federal Rule of Civil Procedure 23(a), 23(b)(1), 23(b)(2), and 23(b)(3).

143. Specifically, Plaintiff proposes the following class definition, subject to amendment as appropriate:

All individuals in the United States whose PII was compromised in the Centennial Bank Data Breach which was announced on or about April 19, 2024 (the "Class").

144. Excluded from the Class are Defendant and its parents or subsidiaries, any entities in which they have a controlling interest, as well as their officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns. Also excluded is any Judge to whom this case is assigned as well as their judicial staff and immediate family members.

145. Plaintiff reserves the right to modify or amend the definition of the proposed Class, as well as add subclasses, before the Court determines whether certification is appropriate.

146. The proposed Class meets the criteria for certification under Rule 23(a), (b)(2), and (b)(3).

147. Numerosity. The Class Members are so numerous that joinder of all members is impracticable. Upon information and belief, Plaintiff believes that the proposed Class includes about two million individuals who have been damaged by Defendant's conduct as alleged herein. The precise number of Class Members is unknown to Plaintiff but may be ascertained from Defendant's records.

148. 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 Defendant engaged in the conduct alleged herein;
- b. Whether Defendant's conduct violated the FTC Act;
- c. When Defendant learned of the Data Breach;
- d. Whether Defendant's response to the Data Breach was adequate;
- e. Whether Defendant unlawfully shared, lost, or disclosed Plaintiff's and Class Members' PII;
- f. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the PII compromised in the Data Breach;
- g. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;
- h. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

- i. Whether Defendant owed duties to Class Members to safeguard their PII;
- j. Whether Defendant breached its duties to Class Members to safeguard their PII;
- k. Whether hackers obtained Class Members' PII via the Data Breach;
- l. Whether Defendant had a legal duty to provide timely and accurate notice of the Data Breach to Plaintiff and the Class Members;
- m. Whether Defendant breached its duties to provide timely and accurate notice of the Data Breach to Plaintiff and Class Members;
- n. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;
- o. What damages Plaintiff and Class Members suffered as a result of Defendant's misconduct;
- p. Whether Defendant's conduct was negligent;
- q. Whether Defendant was unjustly enriched;
- r. Whether Plaintiff and Class Members are entitled to actual and/or statutory damages;
- s. Whether Plaintiff and Class Members are entitled to additional credit or identity monitoring and monetary relief; and
- t. Whether Plaintiff and Class Members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

149. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's PII, like that of every other Class Member, was compromised in the Data Breach. Plaintiff's claims are typical of those of the other Class Members because, inter alia, all Class

Members were injured through the common misconduct of Defendant. Plaintiff is advancing the same claims and legal theories on behalf of herself and all other Class Members, and there are no defenses that are unique to Plaintiff. The claims of Plaintiff and those of Class Members arise from the same operative facts and are based on the same legal theories.

150. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of Class Members. Plaintiff's counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

151. 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 systems and unlawfully accessed and exfiltrated 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.

152. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of this controversy and no unusual difficulties are likely to be encountered in the management of this class action. 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, conducting 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.

153. Class certification is also appropriate under Rule 23(b)(2). Defendant has acted and/or refused to act on grounds generally applicable to the Class such that final injunctive relief and/or corresponding declaratory relief is appropriate as to the Class as a whole.

154. Finally, all members of the proposed Class are readily ascertainable. Defendant has access to the names and addresses and/or email addresses of Class Members affected by the Data Breach. Class Members have already been preliminarily identified and sent a Notice Letter by Defendant.

FIRST CAUSE OF ACTION
NEGLIGENCE AND NEGLIGENCE *PER SE*
(On Behalf of Plaintiff and the Class)

155. Plaintiff restates and incorporates by reference herein all the allegations contained in paragraphs 1 through 154, as if fully set forth herein.

156. Defendant owed a duty under common law to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting their PII in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

157. Defendant's duty to use reasonable care arose from several sources, including but not limited to those described below.

158. Defendant had a common law duty to prevent foreseeable harm to others. This duty existed because Plaintiff and Class Members were the foreseeable and probable victims of any inadequate security practices on the part of Defendant. By collecting and storing PII that is routinely targeted by criminals for unauthorized access, Defendant was obligated to act with reasonable care to protect against these foreseeable threats.

159. Defendant's duty also arose from Defendant's position as a financial institution. Defendant holds itself out as a trusted provider of financial services, and thereby assumes a duty to reasonably protect its customers' sensitive PII information. Indeed, Defendant, as a financial institution, was in a unique and superior position to protect against the harm suffered by Plaintiff and Class Members as a result of the Data Breach.

160. Defendant breached the duties owed to Plaintiff and Class Members and thus was negligent. Defendant breached these duties by, among other things: (a) mismanaging its system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that resulted in the unauthorized access and compromise of PII; (b) mishandling its data security by failing to assess the sufficiency of their safeguards in place to control these risks; (c) failing to design and implement information safeguards to control these risks; (d) failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures; (e) failing to evaluate and adjust its information security program in light of the circumstances alleged herein; (f) failing to detect the breach at the time it began or within a reasonable time thereafter; and (g) failing to follow its own privacy policies and practices published to its customers.

161. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and Class Members, their PII would not have been compromised.

162. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by entities such as Defendant of failing to use reasonable measures to protect PII. Various FTC publications and orders also form the basis of Defendant's duty.

163. Defendant violated Section 5 of the FTCA by failing to use reasonable measures to

protect the PII and not complying with the industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of a data breach involving the PII of its customers.

164. Plaintiff and members of the Class are consumers within the class of persons Section 5 of the FTCA was intended to protect.

165. The harm that has occurred as a result of Defendant's conduct is the type of harm that the FTCA was intended to guard against.

166. Defendant's violation of Section 5 of the FTCA constitutes negligence *per se*.

167. The Safeguards Rule, which implements Section 501(b) of the GLBA, 15 U.S.C. § 6801(b), requires financial institutions to protect the security, confidentiality, and integrity of customer information by developing a comprehensive written information security program that contains reasonable administrative, technical, and physical safeguards.

168. Defendant violated Section 501(b) of the GLBA and the Safeguards Rule by failing to implement and/or inadequately implementing information security policies or procedures such as effective employee training, adequate intrusion detection systems, regular reviews of audit logs and records, and other similar measures to protect the confidentiality of the PII it maintained in its information technology systems.

169. Plaintiff and members of the Class are consumers within the class of persons Section 501(b) of the GLBA and the Safeguards Rule were intended to protect.

170. The harm that has occurred as a result of Defendant's conduct is the type of harm that Section 501(b) of the GLBA and the Safeguards Rule were intended to guard against.

171. Defendant's violation of Section 501(b) of the GLBA and the Safeguards Rule constitutes negligence *per se*.

172. Additionally, Defendant violated its own policies by actively disclosing Plaintiff's and the Class Members' PII; by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' PII; failing to maintain the confidentiality of Plaintiff's and the Class Members' records; and by failing to provide timely notice of the breach of PII to Plaintiff and the Class.

173. As a direct and proximate result of Defendant's negligence, Plaintiff and Class Members have suffered injuries, including, without limitation:

- a. Theft of their PII;
- b. Costs associated with the detection and prevention of identity theft and unauthorized use of the financial accounts;
- c. Costs associated with purchasing credit monitoring and identity theft protection services;
- d. Lowered credit scores resulting from credit inquiries following fraudulent activities;
- e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;
- f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PII being placed in the hands of criminals;
- g. Damages to and diminution in value of their PII entrusted, directly or indirectly, to Defendant with the mutual understanding that Defendant would safeguard Plaintiff's and Class Members' data against theft and not allow access and misuse of their data by others;
- h. Continued risk of exposure to hackers and thieves of their PII, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' data;

- i. Loss of their privacy and confidentiality in their PII;
- j. The erosion of the essential and confidential relationship between Defendant— as a financial services provider – and Plaintiff and Class Members as customers; and
- k. Loss of personal time spent carefully reviewing bills to check for charges for services not received.

174. As a direct and proximate result of Defendant’s negligence, Plaintiff and Class Members are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

SECOND CAUSE OF ACTION
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and the Class)

175. Plaintiff restates and incorporates by reference herein all the allegations contained in paragraphs 1 through 154, as if fully set forth herein.

176. When Plaintiff and members of the Class provided their PII to Defendant, Plaintiff and members of the Class entered into implied contracts with Defendant pursuant to which Defendant agreed to safeguard and protect such information and to timely and accurately notify Plaintiff and Class Members that their data had been breached and compromised.

177. Defendant required Plaintiff and class Members to provide and entrust their PII as a condition of obtaining Defendant’s services.

178. Plaintiff and Class Members would not have provided and entrusted their PII to Defendant in the absence of the implied contract between them and Defendant.

179. Plaintiff and members of the Class fully performed their obligations under the implied contracts with Defendant.

180. Defendant breached the implied contracts it made with Plaintiff and Class Members by failing to safeguard and protect the PII of Plaintiff and members of the Class and by failing to

provide adequate notice about their personal information was compromised in and as a result of the Data Breach.

181. As a direct and proximate result of Defendant's breach of the implied contracts, Plaintiff and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, and/or disgorgement or restitution, in an amount to be proven at trial.

THIRD CAUSE OF ACTION
BREACH OF FIDUCIARY DUTY
(On Behalf of Plaintiff and the Class)

182. Plaintiff restates and incorporates by reference herein all the allegations contained in paragraphs 1 through 154, as if fully set forth herein.

183. Plaintiff and Class Members have an interest, both equitable and legal, in the PII about them that was conveyed to, collected by, and maintained by Defendant and that was ultimately accessed or compromised in the Data Breach.

184. As a financial institution, Defendant has a fiduciary relationship with its customers, like Plaintiff and the Class Members.

185. Because of that fiduciary relationship, Defendant was provided with and stored private and valuable PII related to Plaintiff and the Class, which it was required to maintain in confidence.

186. Defendant owed a fiduciary duty under common law to Plaintiff and Class Members to exercise the utmost care in obtaining, retaining, securing, safeguarding, deleting, and protecting their PII in its possession from being compromised, lost, stolen, accessed by, misused by, or disclosed to unauthorized persons.

187. As a result of the parties' fiduciary relationship, Defendant had an obligation to maintain the confidentiality of Plaintiff's and the Class Members' PII stored in its systems.

188. Customers like Plaintiff and Class Members have a privacy interest in personal financial matters, and Defendant had a fiduciary duty not to disclose financial data concerning its customers.

189. As a result of the parties' relationship, Defendant had possession and knowledge of confidential PII of Plaintiff and Class Members, information not generally known.

190. Plaintiff and Class Members did not consent to nor authorize Defendant to release or disclose their PII to an unknown criminal actor.

191. Defendant breached the duties owed to Plaintiff and Class Members by, among other things: (a) mismanaging its system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that resulted in the unauthorized access and compromise of PII; (b) mishandling its data security by failing to assess the sufficiency of their safeguards in place to control these risks; (c) failing to design and implement information safeguards to control these risks; (d) failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures; (e) failing to evaluate and adjust its information security program in light of the circumstances alleged herein; (f) failing to detect the breach at the time it began or within a reasonable time thereafter; (g) failing to follow its own privacy policies and practices published to its customers; and (h) making an unauthorized and unjustified disclosure and release of Plaintiff and the Class Members' PII and medical records/information to a criminal third party.

192. But for Defendant's wrongful breach of its fiduciary duties owed to Plaintiff and Class Members, their privacy, confidences, and PII would not have been compromised.

193. As a direct and proximate result of Defendant's breach of their fiduciary duties and breach of their confidences, Plaintiff and Class Members have suffered injuries, including:

- a. Theft of their PII;
- b. Costs associated with the detection and prevention of identity theft and unauthorized use of the financial accounts;
- c. Costs associated with purchasing credit monitoring and identity theft protection services;
- d. Lowered credit scores resulting from credit inquiries following fraudulent activities;
- e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;
- f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PII being placed in the hands of criminals;
- g. Damages to and diminution in value of their PII entrusted, directly or indirectly, to Defendant with the mutual understanding that Defendant would safeguard Plaintiff's and Class Members' data against theft and not allow access and misuse of their data by others;
- h. Continued risk of exposure to hackers and thieves of their PII, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' data;
- i. Loss of their privacy and confidentiality in their PII;
- j. The erosion of the essential and confidential relationship between Defendant– as a financial services provider – and Plaintiff and Class Members as customers; and
- k. Loss of personal time spent carefully reviewing bills and statements to check for charges for services not received, as directed to do by Defendant.

194. As a direct and proximate result of Defendant's breach of its fiduciary duty, Plaintiff and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

FOURTH CAUSE OF ACTION
BREACH OF CONFIDENCE
(On Behalf of Plaintiff and the Class)

195. Plaintiff restates and incorporates by reference herein all the allegations contained in paragraphs 1 through 154, as if fully set forth herein.

196. Plaintiff and Class Members have an interest, both equitable and legal, in the PII about them that was conveyed to, collected by, and maintained by Defendant and that was ultimately accessed or compromised in the Data Breach.

197. As a financial service provider, Defendant is in a position of trust and confidence vis-à-vis its customers has a special relationship with its customers, like Plaintiff and the Class Members.

198. Because of that special relationship, Defendant was provided with and stored private and valuable PII related to Plaintiff and the Class, which it was required to maintain in confidence.

199. Plaintiff and the Class provided Defendant with their personal and confidential PII under both the express and/or implied agreement of Defendant to limit the use and disclosure of such PII.

200. Defendant owed a duty to Plaintiff and Class Members to exercise the utmost care in obtaining, retaining, securing, safeguarding, deleting, and protecting their PII in its possession from being compromised, lost, stolen, accessed by, misused by, or disclosed to unauthorized persons.

201. Defendant had an obligation to maintain the confidentiality of Plaintiff's and the Class Members' PII.

202. Plaintiff and Class Members have a privacy interest in their personal financial

matters, and Defendant had a duty not to disclose confidential financial information and records concerning its customers.

203. As a result of the parties' relationship, Defendant had possession and knowledge of confidential PII and confidential personal financial data of Plaintiff and Class Members.

204. Plaintiff's and the Class's PII is not generally known to the public and is confidential by nature.

205. Plaintiff and Class Members did not consent to nor authorize Defendant to release or disclose their PII to an unknown criminal actor.

206. Defendant breached the duties of confidence it owed to Plaintiff and Class Members when Plaintiff's and Class's PII was disclosed to unknown criminal hackers.

207. Defendant breached its duties of confidence by failing to safeguard Plaintiff's and Class Members' PII, including by, among other things: (a) mismanaging its system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that resulted in the unauthorized access and compromise of PII; (b) mishandling its data security by failing to assess the sufficiency of its safeguards in place to control these risks; (c) failing to design and implement information safeguards to control these risks; (d) failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures; (e) failing to evaluate and adjust their information security program in light of the circumstances alleged herein; (f) failing to detect the breach at the time it began or within a reasonable time thereafter; (g) failing to follow its own privacy policies and practices published to its customers; (h) storing PII in an unencrypted and vulnerable manner, allowing its disclosure to hackers; and (i) making an unauthorized and unjustified disclosure and release of Plaintiff and the Class Members' PII and financial records/information to a criminal third party.

208. But for Defendant's wrongful breach of its duty of confidences owed to Plaintiff and Class Members, their privacy, confidences, and PII would not have been compromised.

209. As a direct and proximate result of Defendant's breach of Plaintiff's and the Class's confidences, Plaintiff and Class Members have suffered injuries, including:

- a. The erosion of the essential and confidential relationship between Defendant— as a financial services provider — and Plaintiff and Class Members as customers;
- b. Loss of their privacy and confidentiality in their PII;
- c. Theft of their PII;
- d. Costs associated with the detection and prevention of identity theft and unauthorized use of the financial accounts;
- e. Costs associated with purchasing credit monitoring and identity theft protection services;
- f. Lowered credit scores resulting from credit inquiries following fraudulent activities;
- g. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach — including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;
- h. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PII being placed in the hands of criminals;
- i. Damages to and diminution in value of their PII entrusted, directly or indirectly, to Defendant with the mutual understanding that Defendant would safeguard Plaintiff's and Class Members' data against theft and not allow access and misuse of their data by others;
- j. Continued risk of exposure to hackers and thieves of their PII, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' data;
- k. Loss of personal time spent carefully reviewing statements and records to

check for charges for services not received; and

1. Mental anguish accompanying the loss of confidences and disclosure of their confidential and private PII.

210. Additionally, Defendant received payments from Plaintiff and Class Members for services with the understanding that Defendant would uphold their responsibilities to maintain the confidences of Plaintiff and Class Members' sensitive PII.

211. Defendant breached the confidence of Plaintiff and Class Members when it made an unauthorized release and disclosure of their confidential PII and, accordingly, it would be inequitable for Defendant to retain the benefit at Plaintiff and Class Members' expense.

212. As a direct and proximate result of Defendant's breach of its fiduciary duty of confidence, Plaintiff and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, and/or disgorgement or restitution, in an amount to be proven at trial.

FIFTH CAUSE OF ACTION
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Class)

213. Plaintiff restates and incorporates by reference herein all the allegations contained in paragraphs 1 through 154, as if fully set forth herein.

214. This count is brought in the alternative to Plaintiff's breach of implied contract count above.

215. Plaintiff and Class Members conferred a benefit on Defendant by way of customers' paying Defendant to maintain Plaintiff and Class Members' PII provided as part of Defendant's business as a financial institution.

216. The monies paid to Defendant were supposed to be used by Defendant, in part, to pay for the administrative and other costs of providing reasonable data security and protection to

Plaintiff and Class Members.

217. Defendant failed to provide reasonable security, safeguards, and protections to the personal information of Plaintiff and Class Members, and as a result Defendant was overpaid.

218. Under principles of equity and good conscience, Defendant should not be permitted to retain the money because Defendant failed to provide adequate safeguards and security measures to protect Plaintiff's and Class Members' PII, which they paid for but did not receive.

219. Defendant wrongfully accepted and retained these benefits to the detriment of Plaintiff and Class Members.

220. Defendant's enrichment at the expense of Plaintiff and Class Members is and was unjust.

221. As a result of Defendant's wrongful conduct, as alleged above, Plaintiff and the Class are entitled to restitution and disgorgement of profits, benefits, and other compensation obtained by Defendant, plus attorneys' fees, costs, and interest thereon.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and all other similarly situated, prays for relief as follows:

- a. For an order certifying the Class and naming Plaintiff as the representative of the Classes and Plaintiff's attorneys as Counsel to represent the Classes;
- b. For an order finding in favor of Plaintiff and the Class on all counts asserted herein;
- c. For compensatory, statutory, treble, and/or punitive damages in amounts to be determined by the trier of fact;
- d. For an order of restitution, disgorgement, and all other forms of equitable monetary relief;

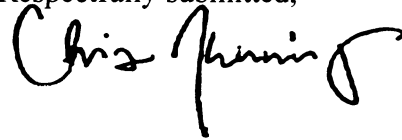
- e. Declaratory and injunctive relief as described herein;
- f. Awarding Plaintiff's reasonable attorneys' fees, costs, and expenses;
- g. Awarding pre- and post-judgment interest on any amounts awarded; and
- h. Awarding such other and further relief as may be just and proper.

JURY TRIAL DEMANDED

A jury trial is demanded on all claims so triable.

Dated: May 1, 2024.

Respectfully submitted,



Christopher D. Jennings
(AR Bar No.: 2006306)
JENNINGS PLLC
PO Box 25972 Little Rock, AR 72221
P: 501-247-6267
E: chris@jenningspllc.com

Jeff Ostrow*
KOPELOWITZ OSTROW
FERGUSON WEISELBERG GILBERT
One West Las Olas Blvd., Suite 500
Fort Lauderdale, Florida 33301
Telephone: 954-525-4100
ostrow@kolawyers.com

**Pro hac vice application forthcoming*

JS 44 (Rev. 03/24)

CIVIL COVER SHEET 4:24-cv-392-JM

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. (SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)

<p>I. (a) PLAINTIFFS Karen Watkins, on behalf of herself and all others similarly situated,</p> <p>(b) County of Residence of First Listed Plaintiff _____ (EXCEPT IN U.S. PLAINTIFF CASES)</p> <p>(c) Attorneys (Firm Name, Address, and Telephone Number) Christopher D. Jennings, Jennings PLLC, P.O. Box 25972, Little Rock, AR, 72221; (501) 247-6267</p>	<p>DEFENDANTS Centennial Bank d/b/a Happy State Bank</p> <p>County of Residence of First Listed Defendant <u>Faulkner County, Ark.</u> (IN U.S. PLAINTIFF CASES ONLY)</p> <p>NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.</p> <p>Attorneys (If Known) Martha Ayers, Table Law, 10201 W. Markham Street, Suite 311, Little Rock, AR</p>
--	---

<p>II. BASIS OF JURISDICTION (Place an "X" in One Box Only)</p> <p><input type="checkbox"/> 1 U.S. Government Plaintiff</p> <p><input type="checkbox"/> 2 U.S. Government Defendant</p> <p><input type="checkbox"/> 3 Federal Question (U.S. Government Not a Party)</p> <p><input checked="" type="checkbox"/> 4 Diversity (Indicate Citizenship of Parties in Item III)</p>	<p>III. CITIZENSHIP OF PRINCIPAL PARTIES (Place an "X" in One Box for Plaintiff and One Box for Defendant)</p> <table style="width:100%;"> <tr> <td style="width:33%;"></td> <td style="width:33%; text-align: center;">PTF</td> <td style="width:33%; text-align: center;">DEF</td> </tr> <tr> <td>Citizen of This State</td> <td style="text-align: center;"><input type="checkbox"/> 1</td> <td style="text-align: center;"><input type="checkbox"/> 1</td> </tr> <tr> <td>Citizen of Another State</td> <td style="text-align: center;"><input checked="" type="checkbox"/> 2</td> <td style="text-align: center;"><input type="checkbox"/> 2</td> </tr> <tr> <td>Citizen or Subject of a Foreign Country</td> <td style="text-align: center;"><input type="checkbox"/> 3</td> <td style="text-align: center;"><input type="checkbox"/> 3</td> </tr> </table> <table style="width:100%;"> <tr> <td style="width:33%;"></td> <td style="width:33%; text-align: center;">PTF</td> <td style="width:33%; text-align: center;">DEF</td> </tr> <tr> <td>Incorporated or Principal Place of Business In This State</td> <td style="text-align: center;"><input type="checkbox"/> 4</td> <td style="text-align: center;"><input checked="" type="checkbox"/> 4</td> </tr> <tr> <td>Incorporated and Principal Place of Business In Another State</td> <td style="text-align: center;"><input type="checkbox"/> 5</td> <td style="text-align: center;"><input type="checkbox"/> 5</td> </tr> <tr> <td>Foreign Nation</td> <td style="text-align: center;"><input type="checkbox"/> 6</td> <td style="text-align: center;"><input type="checkbox"/> 6</td> </tr> </table>		PTF	DEF	Citizen of This State	<input type="checkbox"/> 1	<input type="checkbox"/> 1	Citizen of Another State	<input checked="" type="checkbox"/> 2	<input type="checkbox"/> 2	Citizen or Subject of a Foreign Country	<input type="checkbox"/> 3	<input type="checkbox"/> 3		PTF	DEF	Incorporated or Principal Place of Business In This State	<input type="checkbox"/> 4	<input checked="" type="checkbox"/> 4	Incorporated and Principal Place of Business In Another State	<input type="checkbox"/> 5	<input type="checkbox"/> 5	Foreign Nation	<input type="checkbox"/> 6	<input type="checkbox"/> 6
	PTF	DEF																							
Citizen of This State	<input type="checkbox"/> 1	<input type="checkbox"/> 1																							
Citizen of Another State	<input checked="" type="checkbox"/> 2	<input type="checkbox"/> 2																							
Citizen or Subject of a Foreign Country	<input type="checkbox"/> 3	<input type="checkbox"/> 3																							
	PTF	DEF																							
Incorporated or Principal Place of Business In This State	<input type="checkbox"/> 4	<input checked="" type="checkbox"/> 4																							
Incorporated and Principal Place of Business In Another State	<input type="checkbox"/> 5	<input type="checkbox"/> 5																							
Foreign Nation	<input type="checkbox"/> 6	<input type="checkbox"/> 6																							

IV. NATURE OF SUIT (Place an "X" in One Box Only) Click here for: [Nature of Suit Code Description](#)

<p>CONTRACT</p> <p><input type="checkbox"/> 110 Insurance</p> <p><input type="checkbox"/> 120 Marine</p> <p><input type="checkbox"/> 130 Miller Act</p> <p><input type="checkbox"/> 140 Negotiable Instrument</p> <p><input type="checkbox"/> 150 Recovery of Overpayment & Enforcement of Judgment</p> <p><input type="checkbox"/> 151 Medicare Act</p> <p><input type="checkbox"/> 152 Recovery of Defaulted Student Loans (Excludes Veterans)</p> <p><input type="checkbox"/> 153 Recovery of Overpayment of Veteran's Benefits</p> <p><input type="checkbox"/> 160 Stockholders' Suits</p> <p><input type="checkbox"/> 190 Other Contract</p> <p><input type="checkbox"/> 195 Contract Product Liability</p> <p><input type="checkbox"/> 196 Franchise</p>	<p>TORTS</p> <p>PERSONAL INJURY</p> <p><input type="checkbox"/> 310 Airplane</p> <p><input type="checkbox"/> 315 Airplane Product Liability</p> <p><input type="checkbox"/> 320 Assault, Libel & Slander</p> <p><input type="checkbox"/> 330 Federal Employers' Liability</p> <p><input type="checkbox"/> 340 Marine</p> <p><input type="checkbox"/> 345 Marine Product Liability</p> <p><input type="checkbox"/> 350 Motor Vehicle</p> <p><input type="checkbox"/> 355 Motor Vehicle Product Liability</p> <p><input checked="" type="checkbox"/> 360 Other Personal Injury</p> <p><input type="checkbox"/> 362 Personal Injury - Medical Malpractice</p> <p>PERSONAL INJURY</p> <p><input type="checkbox"/> 365 Personal Injury - Product Liability</p> <p><input type="checkbox"/> 367 Health Care/Pharmaceutical Personal Injury Product Liability</p> <p><input type="checkbox"/> 368 Asbestos Personal Injury Product Liability</p> <p>PERSONAL PROPERTY</p> <p><input type="checkbox"/> 370 Other Fraud</p> <p><input type="checkbox"/> 371 Truth in Lending</p> <p><input type="checkbox"/> 380 Other Personal Property Damage</p> <p><input type="checkbox"/> 385 Property Damage Product Liability</p>	<p>FORFEITURE/PENALTY</p> <p><input type="checkbox"/> 625 Drug Related Seizure of Property 21 USC 881</p> <p><input type="checkbox"/> 690 Other</p> <p>LABOR</p> <p><input type="checkbox"/> 710 Fair Labor Standards Act</p> <p><input type="checkbox"/> 720 Labor/Management Relations</p> <p><input type="checkbox"/> 740 Railway Labor Act</p> <p><input type="checkbox"/> 751 Family and Medical Leave Act</p> <p><input type="checkbox"/> 790 Other Labor Litigation</p> <p><input type="checkbox"/> 791 Employee Retirement Income Security Act</p> <p>IMMIGRATION</p> <p><input type="checkbox"/> 462 Naturalization Application</p> <p><input type="checkbox"/> 465 Other Immigration Actions</p>	<p>BANKRUPTCY</p> <p><input type="checkbox"/> 422 Appeal 28 USC 158</p> <p><input type="checkbox"/> 423 Withdrawal 28 USC 157</p> <p>INTELLECTUAL PROPERTY RIGHTS</p> <p><input type="checkbox"/> 820 Copyrights</p> <p><input type="checkbox"/> 830 Patent</p> <p><input type="checkbox"/> 835 Patent - Abbreviated New Drug Application</p> <p><input type="checkbox"/> 840 Trademark</p> <p><input type="checkbox"/> 880 Defend Trade Secrets Act of 2016</p> <p>SOCIAL SECURITY</p> <p><input type="checkbox"/> 861 HIA (1395ff)</p> <p><input type="checkbox"/> 862 Black Lung (923)</p> <p><input type="checkbox"/> 863 DIWC/DIWW (405(g))</p> <p><input type="checkbox"/> 864 SSID Title XVI</p> <p><input type="checkbox"/> 865 RSI (405(g))</p> <p>FEDERAL TAX SUITS</p> <p><input type="checkbox"/> 870 Taxes (U.S. Plaintiff or Defendant)</p> <p><input type="checkbox"/> 871 IRS—Third Party 26 USC 7609</p>	<p>OTHER STATUTES</p> <p><input type="checkbox"/> 375 False Claims Act</p> <p><input type="checkbox"/> 376 Qui Tam (31 USC 3729(a))</p> <p><input type="checkbox"/> 400 State Reapportionment</p> <p><input type="checkbox"/> 410 Antitrust</p> <p><input type="checkbox"/> 430 Banks and Banking</p> <p><input type="checkbox"/> 450 Commerce</p> <p><input type="checkbox"/> 460 Deportation</p> <p><input type="checkbox"/> 470 Racketeer Influenced and Corrupt Organizations</p> <p><input type="checkbox"/> 480 Consumer Credit (15 USC 1681 or 1692)</p> <p><input type="checkbox"/> 485 Telephone Consumer Protection Act</p> <p><input type="checkbox"/> 490 Cable/Sat TV</p> <p><input type="checkbox"/> 850 Securities/Commodities/Exchange</p> <p><input type="checkbox"/> 890 Other Statutory Actions</p> <p><input type="checkbox"/> 891 Agricultural Acts</p> <p><input type="checkbox"/> 893 Environmental Matters</p> <p><input type="checkbox"/> 895 Freedom of Information Act</p> <p><input type="checkbox"/> 896 Arbitration</p> <p><input type="checkbox"/> 899 Administrative Procedure Act/Review or Appeal of Agency Decision</p> <p><input type="checkbox"/> 950 Constitutionality of State Statutes</p>
---	--	---	---	---

V. ORIGIN (Place an "X" in One Box Only)

1 Original Proceeding

2 Removed from State Court

3 Remanded from Appellate Court

4 Reinstated or Reopened

5 Transferred from Another District (specify)

6 Multidistrict Litigation - Transfer

8 Multidistrict Litigation - Direct File

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing (Do not cite jurisdictional statutes unless diversity):
 28 U.S.C. §1332(d)

Brief description of cause:
 Data Breach

VII. REQUESTED IN COMPLAINT:

CHECK IF THIS IS A CLASS ACTION UNDER RULE 23, F.R.Cv.P.

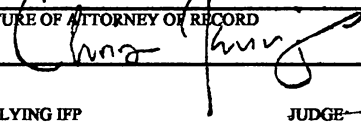
DEMAND \$ 500000

CHECK YES only if demanded in complaint:
 JURY DEMAND: Yes No

VIII. RELATED CASE(S) IF ANY (See instructions):

JUDGE Billy Roy Wilson DOCKET NUMBER 4:23-cv-00333-BRW

DATE May 2, 2024

SIGNATURE OF ATTORNEY OF RECORD 

FOR OFFICE USE ONLY

RECEIPT # _____ AMOUNT _____ APPLYING IFP _____ JUDGE _____ MAG. JUDGE _____