UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF WEST VIRGINIA

JEREMY BASAGIC, individually and on behalf of all others similarly situated, Plaintiff, v. FAIRMONT FEDERAL CREDIT UNION, Defendant.	**Case No.:** 1:25-cv-96 Kleeh **COMPLAINT – CLASS ACTION** **JURY TRIAL DEMANDED**

Plaintiff Jeremy Basagic ("Plaintiff"), on behalf of all others similarly situated, by and through his undersigned counsel, brings this Class Action Complaint against Fairmont Federal Credit Union ("Defendant"). Plaintiff alleges the following upon information and belief based on and the investigation of counsel, except as to those allegations that specifically pertain to Plaintiff, which are alleged upon personal knowledge.

INTRODUCTION

1. Plaintiff and the proposed Class Members bring this class action lawsuit on behalf of all persons who entrusted Defendant with sensitive Personally Identifiable Information ("PII"[1]) and Protected Health Information ("PHI", and collectively, "Private Information) and that were compromised in a data breach (the "Data Breach" or the "Breach").

2. Plaintiff's claims arise from Defendant's failure to properly secure and safeguard Private Information that was entrusted to it, and its accompanying responsibility to store and transfer that information.

[1] Personally identifiable information generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 C.F.R. § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual.

3. Defendant is a credit union company based in West Virginia that offers credit and loan services for individuals and businesses such as savings and checking accounts, home and auto loans, student loans, and business accounts.

4. On January 23, 2024, Defendant became aware that it had experienced a data security incident.[2] Upon learning of this issue, Defendant immediately commenced a prompt and thorough investigation.[3]

5. On or about August 17, 2025, Defendant's investigation concluded, and Defendant determined that one or more of the files accessed and/or acquired by the unauthorized party between September 30, 2023 and October 18, 2023, may contain personal information including, full name, date of birth, address, Social Security number, U.S. Alien registration number, passport number, driver's license or state ID number, military ID number, Tax ID number, non-U.S. national identification number, financial account number, routing number, financial institution name, credit card/debit card number, security code/PIN number, credit card/debit card expiration date, IRS PIN number, treatment information/diagnosis, prescription information, provider name, MRN/patient ID, Medicare/Medicaid number, health insurance policy/subscriber number, other health insurance information, treatment cost information, full access credentials, security questions and answers, and digital signatures.[4]

6. On or around September 11, 2025 – more than a year and a half after being made aware of the Data Breach – Defendant began notifying individuals impacted by the Data Breach.

7. Defendant failed to take precautions designed to keep individuals' Private Information secure.

8. Defendant owed Plaintiff and Class Members a duty to take all reasonable and necessary measures to keep the Private Information collected safe and secure from unauthorized

[2] *Fairmont Federal Credit Union Provides Notice of Data Security Incident*, https://cdn.firstbranchcms.com/kcms-doc/163/91576/FFCU-Website-Substitute-Notice-April-28-2025-35873074.1.pdf (last visited Sept. 18, 2025).
[3] *Id.*
[4] *Id.*

access. Defendant solicited, collected, used, and derived a benefit from the Private Information, yet breached its duty by failing to implement or maintain adequate security practices.

9. Defendant admits that information in its system was accessed by unauthorized individuals, though it provided little information regarding how the Data Breach occurred.

10. The sensitive nature of the data exposed through the Data Breach signifies that Plaintiff and Class Members have suffered irreparable harm. Plaintiff and Class Members have lost the ability to control their private information and are subject to an increased risk of identity theft.

11. Defendant, despite having the financial wherewithal and personnel necessary to prevent the Data Breach, nevertheless failed to use reasonable security procedures and practice appropriate to the nature of the sensitive, unencrypted information it maintained for Plaintiff and Class Members, causing the exposure of Plaintiff's and Class Members' Private Information.

12. As a result of Defendant's inadequate digital security and notice process, Plaintiff's and Class Members' Private Information was exposed to criminals. Plaintiff and the Class Members have suffered and will continue to suffer injuries including: financial losses caused by misuse of their Private Information; the loss or diminished value of their Private Information as a result of the Data Breach; lost time associated with detecting and preventing identity theft; and theft of personal and financial information.

13. Plaintiff brings this action on behalf of all persons whose Private Information was compromised as a result of Defendant's failure to: (i) adequately protect the Private Information of Plaintiff and Class Members; (ii) warn Plaintiff and Class Members of Defendant's inadequate information security practices; (iii) effectively secure hardware containing protected Private Information using reasonable and adequate security procedures free of vulnerabilities and incidents; and (iv) timely notify Plaintiff and Class Members of the Data Breach. Defendant's conduct amounts to at least negligence and violates federal and state statutes.

14. Plaintiff brings this action individually and on behalf of a Nationwide Class of similarly situated individuals against Defendant for: negligence; negligence *per se*; unjust

enrichment, breach of implied contract, and breach of fiduciary duty.

15. Plaintiff seeks to remedy these harms and prevent any future data compromise on behalf of himself and all similarly situated persons whose personal data was compromised and stolen as a result of the Data Breach and who remain at risk due to Defendant's inadequate data security practices.

PARTIES

Plaintiff

16. Plaintiff is a citizen and resident of Fairmont, West Virginia.

Defendant

17. Defendant is a West Virginia based credit union with its principal place of business located at 2 The Credit Union Way, Fairmont, West Virginia, 26554.

JURISDICTION AND VENUE

18. This Court has jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. The number of class members is more than 100 and at least one member of the Class defined below is a citizen of a different state that is diverse from Defendant's citizenship. Thus, minimal diversity exists under 28 U.S.C. § 1332 (d) (2) (A). Defendant has its principal place of business located in this District.

19. This Court has personal jurisdiction over Defendant because Defendant is registered to do business and maintains its principal place of business in this District.

20. Venue is proper in this Court because Defendant's principal place of business is located in this District, and because a substantial part of the events, acts, and omissions giving rise to Plaintiff's claims occurred in this District.

FACTUAL ALLEGATIONS

A. Background on Defendant

21. Defendant is a credit union company based in West Virginia that offers credit and loan services for individuals and businesses such as savings and checking accounts, home and auto loans, student loans, and business accounts.

22. Upon information and belief, Defendant made promises and representations to individuals, including Plaintiff and Class Members, that the Private Information collected from them would be kept safe and confidential, and that the privacy of that information would be maintained.

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

24. As a result of collecting and storing the Private Information of Plaintiff and Class Members for its own financial benefit, Defendant had a continuous duty to adopt and employ reasonable measures to protect Plaintiff's and the Class Members' Private Information from disclosure to third parties.

B. The Data Breach

25. On January 23, 2024, Defendant became aware that it had experienced a data security incident.[5] Upon learning of this issue, Defendant immediately commenced a prompt and thorough investigation.[6]

26. On or about August 17, 2025, Defendant's investigation concluded, and Defendant determined that one or more of the files accessed and/or acquired by the unauthorized party between September 30, 2023 and October 18, 2023, may contain personal information including, full name, date of birth, address, Social Security number, U.S. Alien registration number, passport number, driver's license or state ID number, military ID number, Tax ID number, non-U.S.

[5] *Fairmont Federal Credit Union Provides Notice of Data Security Incident*, https://cdn.firstbranchcms.com/kcms-doc/163/91576/FFCU-Website-Substitute-Notice-April-28-2025-35873074.1.pdf (last visited Sept. 18, 2025).
[6] *Id.*

national identification number, financial account number, routing number, financial institution name, credit card/debit card number, security code/PIN number, credit card/debit card expiration date, IRS PIN number, treatment information/diagnosis, prescription information, provider name, MRN/patient ID, Medicare/Medicaid number, health insurance policy/subscriber number, other health insurance information, treatment cost information, full access credentials, security questions and answers, and digital signatures.[7]

27. On or around September 11, 2025 – more than a year and a half after being made aware of the Data Breach – Defendant began notifying individuals impacted by the Data Breach.

28. Defendant failed to take precautions designed to keep individuals' Private Information secure.

29. Defendant failed to take precautions designed to keep individuals' Private Information secure.

30. While Defendant sought to minimize the damage caused by the Data Breach, it cannot and has not denied that there was unauthorized access to the sensitive Private Information of Plaintiff and Class Members.

31. Individuals affected by the Data Breach are, and remain, at risk that their data will be sold or listed on the dark web and, ultimately, illegally used in the future.

C. Defendant's Failure to Prevent, Identify, and Timely Report the Data Breach

32. Defendant admits that an unauthorized third party accessed IT Network. Defendant failed to take adequate measures to protect its computer systems against unauthorized access.

33. The Private Information that Defendant allowed to be exposed in the Data Breach is the type of private information that Defendant knew or should have known would be the target of cyberattacks.

[7] *Id.*

34. Despite its own knowledge of the inherent risks of cyberattacks, and notwithstanding the FTC's data security principles and practices,[8] Defendant failed to disclose that its systems and security practices were inadequate to reasonably safeguard its past and present customers' Private Information.

35. The FTC directs businesses to use an intrusion detection system to expose a breach as soon as it occurs, monitor activity for attempted hacks, and have an immediate response plan if a breach occurs.[9] Immediate notification of a Data Breach is critical so that those impacted can take measures to protect themselves.

36. Here, Defendant waited more than a year and a half after being made aware of the Data Breach to notify impacted individuals.

D. Defendant Knew—or Should Have Known—of the Risk of a Data Breach

37. It is well known that Private Information is an invaluable commodity and a frequent target of hackers.

38. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in recent years. In light of past high profile data breaches at industry-leading companies, including, for example, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Defendant knew or, if acting as a reasonable business, should have known that the Private Information it collected and maintained would be vulnerable to and targeted by cybercriminals.

39. In 2024, a 3,158 data breaches occurred, exposing approximately 1,350,835,988 sensitive records—a 211% increase year-over-year.[10]

---

[8] Protecting Personal Information: A Guide for Business, FED. TRADE COMM'N (Oct. 2016), https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business. (last visited Sept. 15, 2025).

[9] *Id.*

[10] 2024 Data Breach Annual Report, IDENTITY THEFT RESOURCE CENTER, https://www.idtheftcenter.org/publication/2024-data-breach-report/ (last visited Sept. 15, 2025).

40. Indeed, cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets, so they are aware of and take appropriate measures to prepare for and are able to thwart such an attack.[11]

41. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and Defendant.

42. Despite the prevalence of public announcements of data breaches and data security compromises, and despite its own acknowledgments of data security compromises, and despite its own acknowledgment of its duties to keep Private Information private and secure, Defendant failed to take appropriate steps to protect the Private Information of Plaintiff and Class Members from being compromised.

43. This readily available and accessible information confirms that, prior to the Data Breach, Defendant knew or should have known that (i) ransomware actors were targeting entities such as Defendant, (ii) ransomware gangs were ferociously aggressive in their pursuit of entities such as Defendant, (iii) ransomware gangs were leaking corporate information on dark web portals, and (iv) ransomware tactics included extortion and threatening to release stolen data.

44. In light of the information readily available and accessible before the Data Breach, Defendant knew or should have known that there was a foreseeable risk that Plaintiff's and Class Members' Private Information could be accessed, exfiltrated, and published as the result of a cyberattack. Data breaches are so prevalent in today's society therefore making the risk of experiencing a data breach entirely foreseeable to Defendant.

E. Plaintiff's Experience and Injuries

45. Plaintiff is a customer of Defendant and a data breach victim.

46. As a condition of receiving services, Plaintiff was required to provide his Private

[11] Ben Kochman, FBI, Secret Service Warn of Targeted Ransomware, LAW360 (Nov. 18, 2019), https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware (last visited Sept. 5, 2025).

Information to Defendant.

47. Plaintiff provided his Private Information to Defendant and trusted that the company would use reasonable measures to protect it according to state and federal law.

48. On or around September 11, 2025, Defendant sent Plaintiff a Notice informing him that his Private Information was compromised in the Data Breach.

49. As a result of its inadequate cybersecurity measures and data destruction policies, Defendant exposed Plaintiff's Private Information for theft by cybercriminals and given the purpose of the hack, for sale on the Dark Web.

50. Defendant deprived Plaintiff of the earliest opportunity to guard himself against the Data Breach's effects by failing to promptly notify him about the Data Breach.

51. Plaintiff suffered actual injury from the exposure of his Private Information — which violates his rights to privacy.

52. Plaintiff suffered actual injury in the form of damages to and diminution in the value of his Private Information. After all, Private Information is a form of intangible property—property that Defendant was required to adequately protect.

53. As a result of the Data Breach, Plaintiff has spent time and made reasonable efforts to mitigate its impact, including but not limited to researching the Data Breach, reviewing credit card and financial account statements and monitoring her credit information.

54. Plaintiff will continue to spend considerable time and effort monitoring his accounts to protect himself from identity theft. Plaintiff fears for his personal financial security and uncertainty over what Private Information was exposed. Plaintiff has and is experiencing feelings of anxiety, stress, fear, and frustration because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data

Breach victim that the law contemplates and addresses.

55. And in the aftermath of the Data Breach, Plaintiff has received an uptick in spam text messages, calls, and emails.

56. Plaintiff is now subject to the present and continuing risk of fraud, identity theft, and misuse resulting from his Private Information being placed in the hands of unauthorized third parties. This injury is worsened by Defendant's failure to promptly inform Plaintiff about the Data Breach.

57. Once an individual's Private Information is for sale and accessible on the Dark Web, cybercriminals are able to use the stolen and compromised to gather and steal even more information.[12] Plaintiff's Private Information was compromised as a result of the Data Breach.

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

59. Plaintiff also has a continuing interest in lifetime credit monitoring and identity theft monitoring on account of the Data Breach.

F. Plaintiff and the Class Suffered Common Injuries and Damages Due to Defendant's Conduct

60. Defendant's failure to implement or maintain adequate data security measures for Plaintiff's and Class Members' Private Information directly and proximately injured Plaintiff and Class Members by the resulting disclosure of their Private Information in the Data Breach.

61. Because of Defendant's failure to prevent the Data Breach, Plaintiff and Class members suffered—and will continue to suffer—damages. These damages include, inter alia,

[12] What do Hackers do with Stolen Information, AURA, https://www.aura.com/learn/what-do-hackers-do-with-stolen-information (last visited Sept. 5, 2025).

monetary losses, lost time, anxiety, and emotional distress. Also, they suffered or are at an increased risk of suffering:

a. identity theft and fraud;

b. loss of time to mitigate the risk of identity theft and fraud

c. diminution in value of their Private Information;

d. out-of-pocket costs from trying to prevent, detect, and recover from identity theft and fraud;

e. lost benefit of the bargain and opportunity costs and wages from spending time trying to mitigate the fallout of the Data Breach by, inter alia, preventing, detecting, contesting, and recovering from identify theft and fraud;

f. delay in receipt of tax refund monies;

g. loss of the opportunity to control how their Private Information is used;

h. compromise and continuing publication of their Private Information;

i. unauthorized use of their stolen Private Information;

j. invasion of privacy; and

k. continued risk to their Private Information —which remains in Defendant's possession—and is thus as risk for futures breaches so long as Defendant fails to take appropriate measures to protect the Private Information.

G. Significant Risk of Continued Identity Theft

62. Plaintiff and Class Members are at a heightened risk of identity theft for years to come because of the Data Breach.

63. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 17 C.F.R. § 248.201 (2013).

64. 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." *Id.*

65. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal individuals' personal data to monetize the information. Criminals monetize the data by selling the stolen information on the internet black market (aka the dark web) to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

66. The dark web is an unindexed layer of the internet that requires special software or authentication to access.[13] Criminals in particular favour the dark web as it offers a degree of anonymity to visitors and website publishers. Unlike the traditional or "surface" web, dark web users need to know the web address of the website they wish to visit in advance. For example, on the surface web, the CIA's web address is cia.gov, but on the dark web the CIA's web address is ciadotgov4sjwlzihbbgxnqg3xiyrg7so2r2o3lt5wz5ypk4sxyjstad.onion.[14] This prevents dark web marketplaces from being easily monitored by authorities or accessed by those not in the know.

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

---

[13] What Is the Dark Web? EXPERIAN, available at https://www.experian.com/blogs/ask-experian/what-isthe-dark-web/ (last visited Sept. 15, 2025).
[14] *Id.*

68. The value of Plaintiff's and Class's Private Information on the black market is considerable. Stolen Private Information trades on the black market for years and is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen Private Information can be worth up to $1,000.00 depending on the type of information obtained. Criminals frequently post and sell stolen information openly and directly on the "dark web"—further exposing the information.

69. It can take victims years to discover such identity theft and fraud. This gives criminals plenty of time to sell the Private Information far and wide.

70. 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 to track the victim to attempt other hacking crimes against the individual to obtain more data to perfect a crime.

71. 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 are often the starting point for these additional targeted attacks on the victims.

72. Identity thieves can also use an individual's personal data and Private Information to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's Private Information to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the

victim's information, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant issued in the victim's name.[15]

73. One example of criminals piecing together bits and pieces of compromised Private Information to create comprehensive dossiers on individuals is called "Fullz" packages.[16] These dossiers are both shockingly accurate and comprehensive. With "Fullz" packages, cybercriminals can cross-reference two sources of Private Information to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy to assemble complete dossiers on individuals. For example, they can combine the stolen Private Information, and with unregulated data found elsewhere on the internet (like phone numbers, emails, addresses, etc.).

74. The development of "Fullz" packages means that the Private Information exposed in the Data Breach can easily be linked to data of Plaintiff and the Class that is available on the internet. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the Private Information stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous

[15] Identity Theft and Your Social Security Number, SOCIAL SECURITY ADMINISTRATION, 1 (2018), https://www.ssa.gov/pubs/EN-05-10064.pdf. (last visited Sept. 15, 2025).

[16] "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://krebsonsecuritv.com/2014/09/ medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-firm (last visited Sept. 15, 2025).

operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiff and Class members, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff and other Class members' stolen Private Information is being misused, and that such misuse is fairly traceable to the Data Breach.

75. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses that year, resulting in more than $3.5 billion in losses to individuals and business victims.[17]

76. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good."[18] Yet, Defendant failed to rapidly report to Plaintiff and the Class that their Private Information was stolen. Defendant's failure to promptly and properly notify Plaintiff and Class members of the Data Breach exacerbated Plaintiff and Class members' injury by depriving them of the earliest ability to take appropriate measures to protect their Private Information and take necessary steps to mitigate the harm caused by the Data Breach.

77. Victims of identity theft also often suffer embarrassment, blackmail, or harassment in person or online, and/or experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts.

78. In addition to out-of-pocket expenses that can exceed thousands of dollars and the emotional toll identity theft can take, some victims must spend a considerable time repairing the damage caused by the theft of their Private Information. Victims of new account identity theft will likely have to spend time correcting fraudulent information in their credit reports and continuously

[17] 2019 Internet Crime Report (Feb. 11, 2020) FBI.GOV, https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120 (last visited Sept. 15, 2025).
[18] *Id.*

monitor their reports for future inaccuracies, close existing bank/credit accounts, open new ones, and dispute charges with creditors.

79. Further complicating the issues faced by victims of identity theft, data thieves may wait years before attempting to use the stolen Private Information. To protect themselves, Plaintiff and Class Members will need to remain vigilant for years or even decades to come.

H. Loss of Time to Mitigate the Risk of Identify Theft and Fraud

80. As a result of the recognized risk of identity theft, when a data breach occurs, and an individual is notified by a company that their Private Information was compromised, 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 asset of time has been lost.

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

82. 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 harm.

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

84. 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.[19]

85. Once Private Information is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or contained against future misuse. For this reason, Plaintiff and Class Members will need to maintain these heightened measures for years, and possibly their entire lives, as a result of Defendant's conduct that caused the Data Breach.

I. Diminished Value of Private Information

86. Personal data like Private Information is a valuable property right.[20]

87. 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 Private Information has considerable market value.

88. An active and robust legitimate marketplace for personal information also exists. In 2019, the data brokering industry was worth roughly $200 billion.[21]

89. 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

[19] See Federal Trade Commission, IDENTITYTHEFT.GOV, https://www.identitytheft.gov/Steps (last visited Sept. 15, 2025).
[20] See, e.g., John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII/PHI") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII/PHI, 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) (last visited Sept. 15, 2025).
[21] Shadowy data brokers make the most of their invisibility cloak (Nov. 5, 2019) LA TIMES, https://www.latimes.com/business/story/2019-11-05/column-data-brokers (last visited Sept. 15, 2025).

provides it to marketers or app developers.[22] Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $60 a year.[23]

90. As a result of the Data Breach, Plaintiff's and Class Members' Private Information, which has an inherent market value in both legitimate and black markets, has been damaged and diminished in its value by its unauthorized and likely release onto the dark web, where holds significant value for the threat actors.

91. However, this transfer of value occurred without any consideration paid to Plaintiff or Class Members for their property, resulting in an economic loss. Moreover, the Private Information is now readily available, and the rarity of the data has been lost, thereby causing additional loss of value.

J. Future Cost of Credit and Identify Theft Monitoring is Reasonable and Necessary

92. To date, Defendant has done little to provide Plaintiff and Class Members with relief for the damages they have suffered due to the Data Breach.

93. Given the type of targeted attack in this case and sophisticated criminal activity, the type of information involved, and the modus operandi of cybercriminals, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the dark web for sale and purchase by criminals intending to utilize the Private Information for identity theft crimes— e.g., opening bank accounts in the victims' names to make purchases or to launder money; filing false tax returns; taking out loans or insurance; or filing false unemployment claims.

94. Such fraud may go undetected until debt collection calls commence months, or even

[22] The Personal Data Revolutaion, DATA COUP, https://datacoup.com/ and How it Works, DIGI.ME, https://digi.me/what-is-digime/ (last visited Sept. 5, 2025).
[23] Frequently Asked Questions, NIELSEN COMPUTER & MOBILE PANEL, https://computermobilepanel.nielsen.com/ui/US/en/faqen.html (last visited Sept 15., 2025).

years, later. An individual may not know that her or her information was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

95. Furthermore, the information accessed and disseminated in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, where victims can easily cancel their cards and request a replacement.[24]

96. The information disclosed in this Data Breach is impossible to "close" and difficult, if not impossible, to change.

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

98. The retail cost of credit monitoring and identity theft monitoring can cost $200 or more a year per Class Member. This is a reasonable and necessary cost to protect Class Members from the risk of identity theft that arose from Defendant's Data Breach. This is a future cost for a minimum of five years that Plaintiff and Class Members would not need to bear but for Defendant's failure to safeguard their Private Information.

K. Lost Benefit of the Bargain

99. Furthermore, Defendant's poor data security deprived Plaintiff and Class Members of the benefit of their bargain.

100. When agreeing to provide their Private Information, which was a condition precedent to obtain services from Defendant, Plaintiff and Class Members, as customers,

[24] Jesse Damiani, Your Social Security Number Costs $4 On The Dark Web, New Report Finds, FORBES (Mar. 25, 2020), https://www.forbes.com/sites/jessedamiani/2020/03/25/your-social-securitynumber-costs-4-on-the-dark-web-new-report-finds/?sh=6a44b6d513f1 (last visited Sept. 15, 2025).

understood and expected that they were, in part, paying for services and data security to protect the Private Information they were required to provide.

101. Plaintiff values data security. Indeed, data security is an important consideration of seeking financial services.

102. In 2024, the technology and communications conglomerate Cisco published the results of its multi-year "Consumer Privacy Survey."[25] Therein, Cisco reported the following:

> "For the past six years, Cisco has been tracking consumer trends across the privacy landscape. During this period, privacy has evolved from relative obscurity to a customer requirement with more than 75% of consumer respondents saying they won't purchase from an organization they don't trust with their data."[26]

103. "Privacy has become a critical element and enabler of customer trust, with 94% of organizations saying their customers would not buy from them if they did not protect data properly."[27] 89% of consumers stated that "I care about data privacy."[28] 83% of consumers declared that "I am willing to spend time and money to protect data" and that "I expect to pay more" for privacy.[29]

104. Defendant did not provide the expected data security. Accordingly, Plaintiff and Class Members received services of a lesser value than what they reasonably expected to receive under the bargains struck with Defendant.

L. Defendant Could Have Prevented the Data Breach

105. Data breaches are preventable.[30] As Lucy Thompson wrote in the Data Breach and

---

[25] Privacy Awareness: Consumers Taking Charge to Protect Personal, CISCO, https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-consumer-privacy-report-2024.pdf (last visited Sept. 15, 2025).
[26] *Id.* at 3.
[27] *Id.*
[28] *Id.* at 9.
[29] *Id.*
[30] Lucy L. Thomson, "Despite the Alarming Trends, Data Breaches Are Preventable," in DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012).

Encryption Handbook, "In almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions."[31] She added that "[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised . . . ."[32]

106. "Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures . . . . Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a data breach never occurs." [33]

107. In a Data Breach like the one here, many failures laid the groundwork for the Breach. For example, the FTC has published guidelines that establish reasonable data security practices for businesses. The guidelines also emphasize the importance of having a data security plan, regularly assessing risks to computer systems, and implementing safeguards to control such risks.

108. Additionally, several industry-standard best practices have been identified that—at a minimum—should be implemented by businesses like Defendant.

M. Defendant Failed to Adhere to FTC Guidelines

109. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making. To that end, the FTC has issued numerous guidelines identifying best data security practices that businesses, such as Defendant, should employ to protect against the unlawful exposure of Private Information.

---

[31] *Id.* at 17.
[32] *Id.* at 28.
[33] *Id.*

110. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established guidelines for fundamental data security principles and practices for business. The guidelines explain that businesses should: (i) protect the personal customer information that they keep; (ii) properly dispose of personal information that is no longer needed; (iii) encrypt information stored on computer networks; (iv) understand their network's vulnerabilities; and (v) implement policies to correct security problems.

111. The guidelines also recommend that businesses watch for large amounts of data being transmitted from the system and have a response plan ready in the event of a breach.

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

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

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

N. Defendant Fails with HIPAA Guidelines

115. Defendant is a covered entity under HIPAA (45 C.F.R. § 160.102) and are required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

116. Defendant is subject to the rules and regulations for safeguarding electronic forms of medical information pursuant to the Health Information Technology Act ("HITECH").[34] *See* 42 U.S.C. §17921, 45 C.F.R. § 160.103.

117. HIPAA's Privacy Rule or *Standards for Privacy of Individually Identifiable Health Information* establishes national standards for the protection of health information

118. HIPAA's Privacy Rule or *Security Standards for the Protection of Electronic Protected Health Information* establishes a national set of security standards for protecting health information that is kept or transferred in electronic form.

119. HIPAA requires "compl[iance] with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronic protected health information." 45 C.F.R. § 164.302.

120. "Electronic protected health information" is "individually identifiable health information … that is (i) transmitted by electronic media; maintained in electronic media." 45 C.F.R. § 160.103.

121. HIPAA's Security Rule requires Defendant to do the following:

[34] HIPAA and HITECH work in tandem to provide guidelines and rules for maintaining protected health information. HITECH references and incorporates HIPAA.

a. Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits;

b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;

c. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted; and

d. Ensure compliance by its workforce.

122. HIPAA also requires Defendant to "review and modify the security measures implemented … as needed to continue provision of reasonable and appropriate protection of electronic protected health information." 45 C.F.R. § 164.306(e). Additionally, Defendant is required under HIPAA to "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights." 45 C.F.R. § 164.312(a)(1).

123. HIPAA and HITECH also obligated Defendant to implement policies and procedures to prevent, detect, contain, and correct security violations, and to protect against uses or disclosures of electronic protected health information that are reasonably anticipated but not permitted by the privacy rules. *See* 45 C.F.R. § 164.306(a)(1) and § 164.306(a)(3); *see also* 42 U.S.C. §17902.

124. The HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, also requires Defendant to provide notice of the Data Breach to each affected individual without unreasonable delay.

125. HIPAA requires a covered entity to have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the

covered entity or the requirements of 45 C.F.R. Part 164, Subparts D or E. *See* 45 C.F.R. § 164.530(e).

126. HIPAA requires a covered entity to mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of protected health information in violation of its policies and procedures or the requirements of 45 C.F.R. Part 164, Subpart E by the covered entity or its business associate. *See* 45 C.F.R. § 164.530(f).

127. HIPAA also requires the Office of Civil Rights ("OCR"), within the Department of Health and Human Services ("HHS"), to issue annual guidance documents on the provisions in the HIPAA Security Rule. *See* 45 C.F.R. §§ 164.302-164.318. For example, "HHS has developed guidance and tools to assist HIPAA covered entities in identifying and implementing the most cost effective and appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of e-PHI and comply with the risk analysis requirements of the Security Rule." US Department of Health & Human Services, Security Rule Guidance Material.[35] The list of resources includes a link to guidelines set by the National Institute of Standards and Technology (NIST), which OCR says "represent the industry standard for good business practices with respect to standards for securing e-PHI." US Department of Health & Human Services, Guidance on Risk Analysis.[36]

O. Defendant Failed to Follow Industry Standards

128. Experts studying cybersecurity routinely identify financial corporations as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

129. Several best practices have been identified that—at a minimum—should be implemented by businesses like Defendant. These industry standards include: educating all

[35] http://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html.
[36] https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html

employees regarding cybersecurity; strong passwords; multi-layer security, including firewalls, anti-virus, and anti- malware software; encryption (making data unreadable without a key); multi-factor authentication; backup data; and limiting which employees can access sensitive data.

130. Other industry standard best practices include: installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

131. Moreover, companies should retain personal data only as necessary, with legal justification. Personal data should not be stored beyond the time necessary to achieve its initial purpose of collection. In line with industry standard practices, Defendant should have promptly deleted any data it no longer needed to provide services to Plaintiff and the Class.

132. Upon information and belief, Defendant failed to implement industry-standard cybersecurity measures, including failing to meet the minimum standards of both the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are established standards in reasonable cybersecurity readiness.

133. These frameworks are applicable and accepted industry standards. And by failing to comply with these accepted standards, Defendant opened the door to the criminals—thereby causing the Data Breach.

P. The Harm Caused by the Data Breach Now and Going Forward

128. Victims of data breaches are susceptible to becoming victims of identity theft. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 17 C.F.R. § 248.201(9). When "identity thieves have your personal information, they can drain your bank account, run up charges on your credit cards, open new utility accounts, or get medical treatment on your health insurance."[37]

129. The type of data that may have been accessed and compromised here can be used to perpetrate fraud and identity theft.

130. Plaintiff and Class Members face a substantial risk of identity theft given that their Private Information was compromised in the Data Breach.

131. Stolen Private Information is often trafficked on the "dark web," a heavily encrypted part of the Internet that is not accessible via traditional search engines. Law enforcement has difficulty policing the "dark web" due to this encryption, which allows users and criminals to conceal their identities and online activity.

132. When malicious actors infiltrate companies and copy and exfiltrate the Private Information that those companies store, the stolen information often ends up on the dark web where malicious actors buy and sell that information for profit.[38]

133. For example, when the U.S. Department of Justice announced their seizure of AlphaBay—the largest online "dark market"—in 2017, AlphaBay had more than 350,000 listings, many of which concerned stolen or fraudulent documents that could be used to assume another person's identity."[39] Marketplaces similar to the now-defunct AlphaBay continue to be "awash with [PII] belonging to victims from countries all over the world."[40]

---

[37] Prevention and Preparedness, New York State Police, https://troopers.ny.gov/prevention-and-preparedness (last visited Sept. 15, 2025).

[38] Shining a Light on the Dark Web with Identity Monitoring, IDENTITYFORCE (Dec. 28, 2020) https://www.identityforce.com/blog/shining-light-dark-web-identity-monitoring (last visited Sept. 15, 2025).

[39] Stolen PII & Ramifications: Identity Theft and Fraud on the Dark Web, ARMOR (April 3, 2018), https://res.armor.com/resources/blog/stolen-pii-ramifications-identity-theft-fraud-dark-web/ (last visited Sept. 15, 2025).

[40] *Id.*

134. PII 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. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[41] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[42]

135. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses in 2019, resulting in more than $3.5 billion in losses to individuals and business victims.[43]

136. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good."[44] Defendant did not rapidly report to Plaintiff and Class Members that their Private Information had been stolen. Defendant notified impacted people more than a year and a half after learning of the Data Breach.

137. As a result of the Data Breach, the Private Information of Plaintiff and Class Members has been exposed to criminals for misuse. The injuries suffered by Plaintiff and Class Members, or likely to be suffered as a direct result of Defendant's Data Breach, include: (a) theft of their Private Information; (b) costs associated with the detection and prevention of identity theft; (c) costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the consequences of this Breach; (d) invasion of privacy; (e) the emotional distress, stress, nuisance, and annoyance of responding to, and resulting from, the Data Breach; (f) the actual and/or imminent injury arising from actual and/or potential fraud and identity theft resulting from their personal data being placed in the hands of

---

[41] *Id.*

[42] Bryan Naylor, Victims of Social Security Number Theft Find It's Hard to Bounce Back, NPR (Feb. 9, 2015) https://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last visited Sept. 15, 2025).

[43] 2019 Internet Crime Report Released, FBI (Feb. 11, 2020) https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120#:~:text=IC3%20received%20467%2C361%20complaints%20in,%2Ddelivery%20scams%2C%20and%20extortion (last visited Sept. 15, 2025).

[44] *Id.*

the ill-intentioned hackers and/or criminals; (g) damage to and diminution in value of their personal data entrusted to Defendant with the mutual understanding that Defendant would safeguard their Private Information against theft and not allow access to and misuse of their personal data by any unauthorized third party; and (h) the continued risk to their Private Information, which remains in the possession of Defendant, and which is subject to further injurious breaches so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' Private Information.

138. In addition to a remedy for economic harm, Plaintiff and Class Members maintain an interest in ensuring that their Private Information is secure, remains secure, and is not subject to further misappropriation and theft.

139. Defendant disregarded the rights of Plaintiff and Class Members by (a) intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure that its network servers were protected against unauthorized intrusions; (b) failing to disclose that it did not have adequately robust security protocols and training practices in place to safeguard Plaintiff's and Class Members' Private Information; (c) failing to take standard and reasonably available steps to prevent the Data Breach; (d) concealing the existence and extent of the Data Breach for an unreasonable duration of time; and (e) failing to provide Plaintiff and Class Members prompt and accurate notice of the Data Breach.

140. The actual and adverse effects to Plaintiff and Class Members, including the imminent, immediate, and continuing increased risk of harm for identity theft, identity fraud and/or medical fraud directly or proximately caused by Defendant's wrongful actions and/or inaction and the resulting Data Breach require Plaintiff and Class Members to take affirmative acts to recover their peace of mind and personal security including, without limitation, purchasing credit reporting services, purchasing credit monitoring and/or internet monitoring services, frequently obtaining, purchasing and reviewing credit reports, bank statements, and other similar information, instituting and/or removing credit freezes and/or closing or modifying financial

accounts, for which there is a financial and temporal cost. Plaintiff and other Class Members have suffered, and will continue to suffer, such damages for the foreseeable future.

CLASS ALLEGATIONS

141. Pursuant to Rule 23 of the Federal Rules of Civil Procedure, Plaintiff brings this class action, individually and on behalf of the following Class:

> All persons whose PII/PHI were compromised as a result of the Data Breach (the "Class").

142. Specifically excluded from the Class are Defendant, its officers, directors, agents, trustees, parents, children, corporations, trusts, representatives, principals, servants, partners, joint venturers, or entities controlled by Defendant, and its heirs, successors, assigns, or other persons or entities related to or affiliated with Defendant and/or its officers and/or directors, the judge assigned to this action, and any member of the judge's immediate family.

143. Plaintiff reserves the right to amend the Class definitions above if further investigation and/or discovery reveals that the Class should be expanded, narrowed, divided into subclasses, or otherwise modified in any way.

144. This action may be certified as a class action because it satisfies the numerosity, commonality, typicality, adequacy, and superiority requirements therein.

145. Numerosity: The Class is so numerous that joinder of all Class Members is impracticable. Upon information and belief, the Class is comprised of 187,000 members.[45] The Class is sufficiently numerous to warrant certification.

146. Typicality of Claims: Plaintiff's claims are typical of those of other Class Members because Plaintiff, like the unnamed Class, had his Private Information compromised as a result of the Data Breach. Plaintiff is a member of the Class, and his claims are typical of the claims of the

[45] https://www.wboy.com/news/marion/more-than-187000-affected-by-data-breach-with-fairmont-federal-credit-union/ (last visited Sept. 18, 2025).

members of the Class. The harm suffered by Plaintiff is similar to that suffered by all other Class Members which was caused by the same misconduct by Defendant.

147. Adequacy of Representation: Plaintiff will fairly and adequately represent and protect the interests of the Class. Plaintiff has no interests antagonistic to, nor in conflict with, the Class. Plaintiff has retained competent counsel who are experienced in consumer and commercial class action litigation and who will prosecute this action vigorously.

148. Superiority: A class action is superior to other available methods for the fair and efficient adjudication of this controversy. Because the monetary damages suffered by individual Class Members are relatively small, the expense and burden of individual litigation make it impossible for individual Class Members to seek redress for the wrongful conduct asserted herein. If Class treatment of these claims is not available, Defendant will likely continue its wrongful conduct, will unjustly retain improperly obtained revenues, or will otherwise escape liability for its wrongdoing as asserted herein.

149. Predominant Common Questions: The claims of all Class Members present common questions of law or fact, which predominate over any questions affecting only individual Class Members, including:

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

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

c. Whether Defendant's storage of Plaintiff's and Class Member's Private Information was done in a negligent manner;

d. Whether Defendant had a duty to protect and safeguard Plaintiff's and Class Members' Private Information;

e. Whether Defendant's conduct was negligent;

f. Whether Defendant's conduct violated Plaintiff's and Class Members' privacy;

g. Whether Defendant's conduct violated the statutes as set forth herein;

h. Whether Defendant took sufficient steps to secure its past and present customers Private Information;

i. Whether Defendant was unjustly enriched; and

j. The nature of relief, including damages and equitable relief, to which Plaintiff and Class Members are entitled.

150. Information concerning Defendant's policies is available from Defendant's records.

151. Plaintiff knows of no difficulty which will be encountered in the management of this litigation which would preclude its maintenance as a class action.

152. The prosecution of separate actions by individual members of the Class would run the risk of inconsistent or varying adjudications and establish incompatible standards of conduct for Defendant. Prosecution as a class action will eliminate the possibility of repetitious and inefficient litigation.

153. Given that Defendant had not indicated any changes to its conduct or security measures, monetary damages are insufficient and there is no complete and adequate remedy at law.

CAUSES OF ACTION

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

154. Plaintiff incorporates by reference and re-alleges each and every allegation set forth above as though fully set forth herein.

155. Plaintiff brings this claim individually and on behalf of the Class Members.

156. Defendant knowingly collected, came into possession of, and maintained Plaintiff's and Class Members' Private Information, and had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties.

157. Defendant had a duty to have procedures in place to detect and prevent the loss or unauthorized dissemination of Plaintiff's and Class Members' Private Information.

158. Defendant had, and continues to have, a duty to timely disclose that Plaintiff's and Class Members' Private Information within its possession was compromised and precisely the types of information that were compromised.

159. Defendant owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards, applicable standards of care from statutory authority like Section 5 of the FTC Act, and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected individuals' Private Information.

160. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and its customers. Defendant was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Plaintiff and Class Members from a data breach.

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

162. Defendant breached these duties by failing to exercise reasonable care in safeguarding and protecting Plaintiff's and Class Members' Private Information.

163. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

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

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

c. Failing to periodically ensure that its computer systems and networks had plans in place to maintain reasonable data security safeguards.

164. Defendant, through its actions and/or omissions, unlawfully breached its duties to Plaintiff and Class Members by failing to exercise reasonable care in protecting and safeguarding Plaintiff's and Class Members' Private Information within Defendant's possession.

165. Defendant, through its actions and/or omissions, unlawfully breached its duties to Plaintiff and Class Members by failing to have appropriate procedures in place to detect and prevent dissemination of Plaintiff's and Class Members' Private Information.

166. Defendant, through its actions and/or omissions, unlawfully breached its duty to timely disclose to Plaintiff and Class Members that the Private Information within Defendant's possession might have been compromised and precisely the type of information compromised.

167. Defendant breached the duties set forth in 15 U.S.C. § 45, the FTC guidelines, the National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity, and other industry guidelines. In violation of 15 U.S.C. § 45, Defendant failed to implement proper data security procedures to adequately and reasonably protect Plaintiff's and Class Members' Private Information. In violation of the FTC guidelines, *inter alia,* Defendant did not protect the Private Information it keeps; failed to properly dispose of personal information that was no longer needed; failed to encrypt information stored on computer networks; lacked the requisite understanding of its networks' vulnerabilities; and failed to implement policies to correct security issues.

168. Similarly, under HIPAA, Defendant had a duty to follow HIPAA standards for privacy and security practices—as to protect Plaintiff's and Class Members' PHI.

169. Defendant violated its duty under HIPAA by failing to use reasonable measures to protect its PHI and by not complying with applicable regulations detailed *supra*. Here too, Defendant's conduct was particularly unreasonable given the nature and amount of PHI that Defendant collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

170. It was foreseeable that Defendant's failure to use reasonable measures to protect Plaintiff's and Class Members' Private Information would result in injury to Plaintiff and Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches.

171. It was foreseeable that the failure to adequately safeguard Plaintiff's and Class Members' Private Information would result in injuries to Plaintiff and Class Members.

172. Defendant's breach of duties owed to Plaintiff and Class Members caused Plaintiff's and Class Members' Private Information to be compromised.

173. But for Defendant's negligent conduct and breach of the above-described duties owed to Plaintiff and Class Members, their Private Information would not have been compromised.

174. As a result of Defendant's failure to timely notify Plaintiff and Class Members that their Private Information had been compromised, Plaintiff and Class Members are unable to take the necessary precautions to mitigate damages by preventing future fraud.

175. As a result of Defendant's negligence and breach of duties, Plaintiff and Class Members are in danger of imminent harm in that their Private Information, which is still in the possession of third parties, will be used for fraudulent purposes, and Plaintiff and Class Members have and will suffer damages including: a substantial increase in the likelihood of identity theft; the compromise, publication, and theft of their personal information; loss of time and costs associated with the prevention, detection, and recovery from unauthorized use of their personal information; the continued risk to their personal information; future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the personal information compromised as a result of the Data Breach; and overpayment for the services or products that were received without adequate data security.

COUNT II
NEGLIGENCE *PER SE*
(On Behalf of Plaintiff and the Class)

176. Plaintiff incorporates by reference and re-alleges each and every allegation set forth above as though fully set forth herein.

177. Pursuant to Section 5 of the FTCA, Defendant had a duty to provide fair and adequate computer systems and data security to safeguard the Private Information of Plaintiff and Class Members.

178. Pursuant to HIPAA, 42 U.S.C. § 1302(d), *et seq*., Defendant had a duty to implement reasonable safeguards to protect Plaintiff and Class Members' Private Information.

179. Specifically, pursuant to HIPAA, Defendant had a duty to render the electronic PHI it maintained unusable, unreadable, or indecipherable to unauthorized individuals by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without the use of a confidential process or key." *See* definition of "encryption" at 45 C.F.R. § 164.304.

180. Defendant breached its duties to Plaintiff and Class Members under the FTCA and HIPAA by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff and Class Members' Private Information.

181. Specifically, Defendant breached its duties by failing to employ industry-standard cybersecurity measures in order to comply with the FTCA, including but not limited to proper segregation, access controls, password protection, encryption, intrusion detection, secure destruction of unnecessary data, and penetration testing.

182. The FTCA prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice of failing to use reasonable measures to protect PII and PHI (such as the Private Information compromised in the Data Breach). The FTC rulings and publications described above, together with the industry-standard cybersecurity measures set forth herein, form part of the basis of Defendant's duty in this regard.

183. Defendant also violated the FTCA and HIPAA by failing to use reasonable measures to protect the Private Information of Plaintiff and the Class and by not complying with applicable industry standards, as described herein.

184. It was reasonably foreseeable, particularly given the growing number of data breaches of Private Information, that the failure to reasonably protect and secure Plaintiff and Class Members' Private Information in compliance with applicable laws would result in an unauthorized third-party gaining access to Defendant's networks, databases, and computers that stored Plaintiff's and Class Members' unencrypted Private Information.

185. Plaintiff and Class Members are within the class of persons that the FTCA and HIPAA are intended to protect and Defendant's failure to comply with both constitutes negligence *per se*.

186. Plaintiff and Class Members' Private Information constitutes personal property that was stolen due to Defendant's negligence, resulting in harm, injury, and damages to Plaintiff and Class Members.

187. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and the Class have suffered, and continue to suffer, injuries and damages arising from the unauthorized access of their Private Information, including but not limited to damages from the lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives.

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

189. In addition to monetary relief, Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiff and Class Members.

COUNT III
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Class)

190. Plaintiff incorporates by reference and re-alleges each and every allegation set forth above as though fully set forth herein.

191. Plaintiff and Class Members conferred a benefit upon Defendant by providing Defendant with their Private Information.

192. Defendant appreciated or had knowledge of the benefits conferred upon itself by Plaintiff. Defendant also benefited from the receipt of Plaintiff's and Class Members' Private Information.

193. Under principles of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiff's and the Class Members' Private Information because Defendant failed to adequately protect their Private Information. Plaintiff and the proposed Class would not have provided their Private Information to Defendant had they known Defendant would not adequately protect their Private Information.

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

COUNT IV
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and the Class)

195. Plaintiff incorporates by reference and re-alleges each and every allegation set forth above as though fully set forth herein.

196. Plaintiff and the Class provided and entrusted their Private Information to Defendant. Plaintiff and the Class provided their Private Information to Defendant as part of Defendant's regular business practices.

197. In so doing, Plaintiff and the Class entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such information, to keep such information

secure and confidential, and to timely and accurately notify Plaintiff and the Class if their data had been breached and compromised or stolen, in return for the business services provided by Defendant. Implied in these exchanges was a promise by Defendant to ensure that the Private Information of Plaintiff and Class Members in its possession was secure.

198. Pursuant to these implied contracts, Plaintiff and Class Members provided Defendant with their Private Information. In exchange, Defendant agreed to, among other things, and Plaintiff and the Class understood that Defendant would: (1) provide services to Plaintiff sand Class Members'; (2) take reasonable measures to protect the security and confidentiality of Plaintiff and Class Members' Private Information; and (3) protect Plaintiff and Class Members' Private Information in compliance with federal and state laws and regulations and industry standards.

199. Implied in these exchanges was a promise by Defendant to ensure the Private Information of Plaintiff and Class Members in its possession was only used to provide the agreed-upon reasons, and that Defendant would take adequate measures to protect Plaintiff and Class Members' Private Information.

200. A material term of this contract is a covenant by Defendant that it would take reasonable efforts to safeguard that information. Defendant breached this covenant by allowing Plaintiff and Class Members' Private Information to be accessed in the Data Breach.

201. Indeed, implicit in the agreement between Defendant and Plaintiff and Class Members was the obligation that both parties would maintain information confidentially and securely.

202. These exchanges constituted an agreement and meeting of the minds between the parties.

203. When the parties entered into an agreement, mutual assent occurred. Plaintiff and Class Members would not have disclosed their Private Information to Defendant but for the prospect of utilizing Defendant services. Conversely, Defendant presumably would not have taken Plaintiff and Class Members' Private Information if it did not intend to provide Plaintiff and Class Members with its services.

204. Defendant was therefore required to reasonably safeguard and protect the Private Information of Plaintiff and Class Members from unauthorized disclosure and use.

205. Plaintiff and Class Members would not have entrusted their Private Information to Defendant in the absence of their implied contracts with Defendant and would have instead retained the opportunity to control their Private Information.

206. Defendant breached the implied contracts with Plaintiff and Class Members by failing to reasonably safeguard and protect Plaintiff and Class Members' Private Information.

207. Defendant's failure to implement adequate measures to protect the Private Information of Plaintiff and Class Members violated the purpose of the agreement between the parties.

208. As a proximate and direct result of Defendant's breaches of its implied contracts with Plaintiff and Class Members, Plaintiff and the Class Members suffered damages as described in detail above.

COUNT V
BREACH OF FIDUCIARY DUTY
(On Behalf of Plaintiff and the Class)

209. Plaintiff incorporates by reference and re-alleges each and every allegation set forth above as though fully set forth herein.

210. Defendant became guardian of Plaintiff's and Class Members' Private Information, creating a special relationship between Defendant and Plaintiff and Class Members.

211. As such, Defendant became a fiduciary by its undertaking and guardianship of the Private Information, to act primarily for Plaintiff and Class Members, (1) for the safeguarding of Plaintiff's and Class Members' Private Information; (2) to timely notify Plaintiff and Class Members of a Data Breach and disclosure; and (3) to maintain complete and accurate records of what information (and where) Defendant did and does store.

212. Defendant has a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of Defendant's relationship with its customers, in particular, to keep secure their Private Information.

213. Defendant breached its fiduciary duties to Plaintiff and Class Members by failing to encrypt and otherwise protect the integrity of the systems containing Plaintiff's and Class Members' Private Information.

214. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by failing to timely notify and/or warn Plaintiff and Class Members of the Data Breach.

215. Defendant breached its fiduciary duties to Plaintiff and Class Members by otherwise failing to safeguard Plaintiff's and Class Members' Private Information.

216. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to:

a. actual identity theft;

b. the compromise, publication, and/or theft of their Private Information;

c. out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Private Information;

d. lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft;

e. the continued risk to their Private Information, 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 Private Information in its continued possession;

f. future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the rest of the lives of Plaintiff and Class Members; and

g. the diminished value of Defendant's services they received.

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

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all others similarly situated, seeks judgment against Defendant, as follows:

(a) For an order determining that this action is properly brought as a class action and certifying Plaintiff as the representative of the Class and his counsel as Class Counsel;

(b) For an order declaring that Defendant's conduct violates the laws referenced herein;

(c) For an order finding in favor of Plaintiff and the Class on all counts asserted herein;

(d) For damages in amounts to be determined by the Court and/or jury;

(e) For an award of statutory damages or penalties to the extent available;

(f) For pre-judgment interest on all amounts awarded;

(g) For an order of restitution and all other forms of monetary relief; and

(h) Such other and further relief as the Court deems necessary and appropriate.

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury of all claims in this Class Action Complaint so triable.

Dated: September 22, 2025 By:

/s/ Rodney A. Smith

Rodney A. Smith (WVSB # 9750)
M. Alex Urban (WVSB # 13480)
ROD SMITH LAW PLLC
108 ½ Capitol Street, Suite 300
Charleston, WV 25301
Telephone: (304) 342-0550
Facsimile: (304) 344-5529
rod@LawWV.com
aurban@LawWV.com

Casondra Turner (*pro hac vice* forthcoming)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN PLLC
800 S. Gay Street, Suite 1100
Knoxville, TN 37929
Telephone: (866) 252-0878
Fax: (771) 772-3086
cturner@milberg.com

Attorneys for Plaintiff and the Proposed Class

JS 44 (Rev. 03/24)

CIVIL COVER SHEET

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.)*

I. (a) PLAINTIFFS

JEREMY BASAGIC, individually and on behalf of all others similarly situated

(b) County of Residence of First Listed Plaintiff Marion
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys *(Firm Name, Address, and Telephone Number)*
Rod Smith Law PLLC
108 1/2 Capitol St., Ste. 300, Charleston, WV 25301
304-342-0550

DEFENDANTS

FAIRMONT FEDERAL CREDIT UNION

County of Residence of First Listed Defendant Marion
(IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

Attorneys *(If Known)*

II. BASIS OF JURISDICTION *(Place an "X" in One Box Only)*

- ☐ 1 U.S. Government Plaintiff
- ☐ 3 Federal Question *(U.S. Government Not a Party)*
- ☐ 2 U.S. Government Defendant
- ☒ 4 Diversity *(Indicate Citizenship of Parties in Item III)*

III. CITIZENSHIP OF PRINCIPAL PARTIES *(Place an "X" in One Box for Plaintiff and One Box for Defendant)*

(For Diversity Cases Only)

	PTF	DEF		PTF	DEF
Citizen of This State	☒ 1	☐ 1	Incorporated *or* Principal Place of Business In This State	☐ 4	☒ 4
Citizen of Another State	☐ 2	☐ 2	Incorporated *and* Principal Place of Business In Another State	☐ 5	☐ 5
Citizen or Subject of a Foreign Country	☐ 3	☐ 3	Foreign Nation	☐ 6	☐ 6

IV. NATURE OF SUIT *(Place an "X" in One Box Only)*

Click here for: Nature of Suit Code Descriptions.

CONTRACT
- ☐ 110 Insurance
- ☐ 120 Marine
- ☐ 130 Miller Act
- ☐ 140 Negotiable Instrument
- ☐ 150 Recovery of Overpayment & Enforcement of Judgment
- ☐ 151 Medicare Act
- ☐ 152 Recovery of Defaulted Student Loans (Excludes Veterans)
- ☐ 153 Recovery of Overpayment of Veteran's Benefits
- ☐ 160 Stockholders' Suits
- ☐ 190 Other Contract
- ☐ 195 Contract Product Liability
- ☐ 196 Franchise

TORTS

PERSONAL INJURY
- ☐ 310 Airplane
- ☐ 315 Airplane Product Liability
- ☐ 320 Assault, Libel & Slander
- ☐ 330 Federal Employers' Liability
- ☐ 340 Marine
- ☐ 345 Marine Product Liability
- ☐ 350 Motor Vehicle
- ☐ 355 Motor Vehicle Product Liability
- ☒ 360 Other Personal Injury
- ☐ 362 Personal Injury - Medical Malpractice

PERSONAL INJURY
- ☐ 365 Personal Injury - Product Liability
- ☐ 367 Health Care/ Pharmaceutical Personal Injury Product Liability
- ☐ 368 Asbestos Personal Injury Product Liability

PERSONAL PROPERTY
- ☐ 370 Other Fraud
- ☐ 371 Truth in Lending
- ☐ 380 Other Personal Property Damage
- ☐ 385 Property Damage Product Liability

FORFEITURE/PENALTY
- ☐ 625 Drug Related Seizure of Property 21 USC 881
- ☐ 690 Other

LABOR
- ☐ 710 Fair Labor Standards Act
- ☐ 720 Labor/Management Relations
- ☐ 740 Railway Labor Act
- ☐ 751 Family and Medical Leave Act
- ☐ 790 Other Labor Litigation
- ☐ 791 Employee Retirement Income Security Act

IMMIGRATION
- ☐ 462 Naturalization Application
- ☐ 465 Other Immigration Actions

BANKRUPTCY
- ☐ 422 Appeal 28 USC 158
- ☐ 423 Withdrawal 28 USC 157

INTELLECTUAL PROPERTY RIGHTS
- ☐ 820 Copyrights
- ☐ 830 Patent
- ☐ 835 Patent - Abbreviated New Drug Application
- ☐ 840 Trademark
- ☐ 880 Defend Trade Secrets Act of 2016

SOCIAL SECURITY
- ☐ 861 HIA (1395ff)
- ☐ 862 Black Lung (923)
- ☐ 863 DIWC/DIWW (405(g))
- ☐ 864 SSID Title XVI
- ☐ 865 RSI (405(g))

FEDERAL TAX SUITS
- ☐ 870 Taxes (U.S. Plaintiff or Defendant)
- ☐ 871 IRS—Third Party 26 USC 7609

OTHER STATUTES
- ☐ 375 False Claims Act
- ☐ 376 Qui Tam (31 USC 3729(a))
- ☐ 400 State Reapportionment
- ☐ 410 Antitrust
- ☐ 430 Banks and Banking
- ☐ 450 Commerce
- ☐ 460 Deportation
- ☐ 470 Racketeer Influenced and Corrupt Organizations
- ☐ 480 Consumer Credit (15 USC 1681 or 1692)
- ☐ 485 Telephone Consumer Protection Act
- ☐ 490 Cable/Sat TV
- ☐ 850 Securities/Commodities/ Exchange
- ☐ 890 Other Statutory Actions
- ☐ 891 Agricultural Acts
- ☐ 893 Environmental Matters
- ☐ 895 Freedom of Information Act
- ☐ 896 Arbitration
- ☐ 899 Administrative Procedure Act/Review or Appeal of Agency Decision
- ☐ 950 Constitutionality of State Statutes

REAL PROPERTY
- ☐ 210 Land Condemnation
- ☐ 220 Foreclosure
- ☐ 230 Rent Lease & Ejectment
- ☐ 240 Torts to Land
- ☐ 245 Tort Product Liability
- ☐ 290 All Other Real Property

CIVIL RIGHTS
- ☐ 440 Other Civil Rights
- ☐ 441 Voting
- ☐ 442 Employment
- ☐ 443 Housing/ Accommodations
- ☐ 445 Amer. w/Disabilities - Employment
- ☐ 446 Amer. w/Disabilities - Other
- ☐ 448 Education

PRISONER PETITIONS

Habeas Corpus:
- ☐ 463 Alien Detainee
- ☐ 510 Motions to Vacate Sentence
- ☐ 530 General
- ☐ 535 Death Penalty

Other:
- ☐ 540 Mandamus & Other
- ☐ 550 Civil Rights
- ☐ 555 Prison Condition
- ☐ 560 Civil Detainee - Conditions of Confinement

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)***:
2 C.F.R. § 200.79

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 $

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

VIII. RELATED CASE(S) IF ANY

(See instructions): JUDGE _____ DOCKET NUMBER _____

DATE
September 22, 2025

SIGNATURE OF ATTORNEY OF RECORD
/s/ Rodney A. Smith

FOR OFFICE USE ONLY

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