IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF WEST VIRGINIA

RICHARD BUTLER, TIMOTHY KNOTTS, individually and on behalf of all others similarly situated,

Plaintiff,

v.

FAIRMONT FEDERAL CREDIT UNION,

Defendant.

Civil Action No. 1:25-cv-94 Kleeh

JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiffs Richard Butler and Timothy Knotts (together "Plaintiffs") bring this Class Action Complaint on behalf of themselves, and all others similarly situated, against Defendant Fairmont Federal Credit Union ("FFCU" or "Defendant"), alleging as follows based upon information and belief and investigation of counsel, except as to the allegations specifically pertaining to them, which are based on personal knowledge:

NATURE OF THE CASE

1. Plaintiffs bring this class action against FFCU for its failure to properly secure and safeguard Plaintiffs' and other similarly situated current and former customers' ("Class Members") sensitive information, including *inter alia*, 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, full access credentials,

security questions and answers, and digital signatures (collectively personally identifiable information ("PII")).[1]

2. In addition, Plaintiffs also bring this class action against FFCU for its failure to properly secure and safeguard Plaintiffs' and Class Members' protected health information ("PHI") including health insurance policy/subscriber number, treatment information/diagnosis, prescription information, provider name, MRN/patient ID, and Medicare/Medicaid number.[2]

3. PII and PHI are collectively referred to as "Private Information."

4. Fairmont Federal Credit Union is a federally chartered financial institution providing banking services to individuals and businesses. According to its website, FFCU is "one of the fastest growing credit unions in West Virginia with nearly $475,000,000 in assets."[3]

5. Plaintiffs and Class Members are required to provide Defendant with their Private Information and/or the Private Information of their family members. Because of this, FFCU has a duty to secure, maintain, protect, and safeguard the Private Information that it collects and stores against unauthorized access and disclosure through reasonable and adequate data security measures.

6. Despite FFCU's duty to safeguard the Private Information of its current and previous customers, Plaintiffs' and Class Members' Private Information was compromised in a

[1] *See* FFCU – 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 September 15, 2025).
[2] *Id.*
[3] https://www.fairmontfcu.com/about-us/about-fairmont-fcu.html (last visited September 15, 2025).

data breach when, on or about September 30, 2023, Defendant had experienced a data security incident (the "Data Breach").[4]

7. The data breach occurred in part because FFCU stored Plaintiffs' and Class Members' Private Information in an unencrypted, Internet-accessible environment.

8. After FFCU discovered the Data Breach on or about January 23, 2024, it conducted an investigation which concluded on August 17, 2025, "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..."[5]

9. Despite learning about the breach on January 23, 2024, FFCU incredibly waited over a year and a half until September 11, 2025 to begin notifying impacted individuals of the unauthorized access.[6]

10. Based on publicly available information, the Private Information impacted by the Data Breach includes a wide swath of highly sensitive information belonging to FFCU's current and former customers, as well as certain of their family members, including their 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

---

[4] *See* FFCU – 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 September 15, 2025).
[5] *Id.*
[6] *Data Breach Notifications*, Office of the Maine Attorney General, https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/75c92a2c-3791-47c6-84f7-87b34fab952d.html (last visited September 15, 2025)

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]

11. As a direct and proximate result of Defendant's failure to implement and follow basic security procedures, Plaintiffs' and Class Members' Private Information is now exposed to cybercriminals.

12. Plaintiffs and Class Members are now at a significantly increased and certainly impending risk of fraud, identity theft, intrusion of their health privacy, and similar forms of criminal mischief, risk which may last for the rest of their lives. Consequently, Plaintiffs and Class Members must devote substantially more time, money, and energy to protect themselves, to the extent possible, from these crimes.

13. Plaintiffs, on behalf of themselves and all others similarly situated, allege claims for negligence, breach of implied contract, unjust enrichment and declaratory judgment arising from the Data Breach. Plaintiffs seek damages and injunctive relief, including the adoption reasonably sufficient practices to safeguard the Private Information in Defendant's custody to prevent incidents like the Data Breach from reoccurring in the future, and for Defendant to provide identity theft protective services to Plaintiffs and Class Members for their lifetimes.

PARTIES

14. Plaintiff Butler is an adult, who at all relevant times, was a resident and citizen of the State of North Carolina. Plaintiff received a data breach notice informing him that his Private Information provided to FFCU was compromised during the Data Breach. Prior to receiving any

[7] *See* FFCU – 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 September 15, 2025).

notice of the Breach, Plaintiff Butler had twenty-five thousand dollars ($25,000) fraudulently wired from his account to a third-party account.

15. Plaintiff Knotts is an adult, who at all relevant times, was a resident and citizen of the State of West Virginia. Plaintiff received a data breach notice informing him that his Private Information provided to FFCU was compromised during the Data Breach.

16. In addition to Plaintiff Butler having funds wired from his account, Plaintiffs have suffered actual injury from having their Private Information exposed and/or stolen as a result of the Data Breach, including: (a) required mitigation efforts, including researching the Data Breach and needing to monitor their financial statements to ensure their information is not used for identity theft and fraud; (b) damages to and diminution of the value of their Private Information, a form of intangible property that loses value when it falls into the hands of criminals; (c) loss of privacy; and (d) continuous imminent and impending injury raising from increased risk of financial identity theft and fraud.

17. As a direct and proximate result of the Data Breach, Plaintiffs have also received a significant increase in spam calls and is at an increased risk to continue to receive spam calls since the Data Breach.

18. As a result of the Data Breach, Plaintiffs will continue to be at a substantial and certainly impending risk for fraud and identity theft, and their attendant damages, for years to come.

19. Defendant Fairmont Federal Credit Union is federally chartered credit union with its principal office located at 2 The Credit Union Way, Fairmont, West Virginia 26554.

JURISDICTION AND VENUE

20. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1332(d)(2)(A) because this case is a class action where the aggregate claims of all members of the proposed class are in excess of $5,000,000.00, exclusive of interest and costs, there are 100 or more members of the proposed class, and at least one member of the proposed class is a citizen of a state different than Defendant.

21. This Court has personal jurisdiction over Defendant because a substantial part of the events, omissions, and acts giving rise to the claims herein occurred in this District and Defendant resides in this District.

22. Pursuant to 28 U.S.C. § 1391, this Court is the proper venue for this action because a substantial part of the events, omissions, and acts giving rise to the claims herein occurred in this District and Defendant resides in this District.

FACTUAL BACKGROUND

23. Defendant is a federally chartered, not-for-profit financial cooperative offering banking services such as checking and savings accounts, loans, and other financial products to members across Marion County and nearby communities.

24. Plaintiffs and Class Members are and/or were customers of Defendant.

25. As a condition of obtaining services from Defendant, Plaintiffs and Class Members directly or indirectly entrusted FFCU with their sensitive Private Information.

26. Plaintiffs and Class Members value the confidentiality of their Private Information and, according, have taken reasonable steps to maintain the confidentiality of their Private Information.

27. In turning over their Private Information, Plaintiffs and Class Members reasonably expected that their provider would safeguard their highly sensitive information.

28. By obtaining, collecting, and storing Plaintiffs' and Class Members' Private Information, FFCU assumed equitable and legal duties to safeguard Plaintiffs' and Class Members' highly sensitive information, to only use this information for business purposes, and to only make authorized disclosures.

29. Despite these duties, FFCU failed to implement reasonable data security measures to protect Plaintiffs' and Class Members' Private Information and ultimately allowed threat actors to breach its computer systems and exfiltrate Plaintiffs' and Class Members' Private Information.

THE VALUE OF PRIVATE INFORMATION AND EFFECTS OF UNAUTHORIZED DISCLOSURE

30. FFCU understood that the Private Information it collects was highly sensitive and of significant value to those who would use it for wrongful purposes.

31. FFCU also knew that a breach of its computer systems, and exposure of the Private Information stored therein, would result in the increased risk of identity theft and fraud against the individuals whose Private Information was compromised.

32. These risks are not theoretical; in recent years, numerous high-profile breaches have occurred at business such as Equifax, Facebook, Yahoo, Marriott, Anthem, and many others.

33. Private Information has considerable value and constitutes an enticing and well-known target to hackers. Hackers can easily sell stolen data as there has been "proliferation of open and anonymous cybercrime forums on the Dark Web that serve as a bustling marketplace for such commerce."[8]

[8] 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/ (last accessed September 15, 2025).

34. As the FTC recognizes, identity thieves can use this information to commit an array of crimes including identity theft, and medical and financial fraud.[9]

35. 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 U.S. 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.[10]

36. Indeed, a 2022 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."[11]

37. In tandem with the increase in data breaches, the rate of identity theft complaints has also increased over the past few years. For instance, in 2017, 2.9 million people reported some form of identity fraud compared to 5.7 million people in 2021.[12]

38. The ramifications of FFCU's failure to keep Plaintiffs' and Class Members' Private Information secure are long-lasting and severe. Once Private Information is stolen, fraudulent use

---

[9] https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft (last accessed September 15, 2025).
[10] *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/ (last accessed September 15, 2025).
[11] 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 (last accessed September 15, 2025).
[12] *Insurance Information Institute, Facts + Statistics: Identity theft and cybercrime*, Insurance Information Institute, https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime#Identity%20Theft%20And%20Fraud%20Reports,%202015-2019%20, (last accessed September 15, 2025).

of that information and damage to victims may continue for years. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches: "[I]n some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the [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."[13]

39. Even if stolen Private Information 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 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.

40. The specific types of personal data compromised in the Data Breach makes the information particularly valuable to thieves and leaves Plaintiffs and other Class Members especially vulnerable to identity theft, tax fraud, medical fraud, credit and bank fraud, and more.

41. **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

[13] U.S. Gov't Accountability Office, Report to Congressional Requesters, Personal Information, June 2007: https://www.gao.gov/new.items/d07737.pdf, (last accessed September 15, 2025).

the person's relationships with government agencies and any number of private companies in order to update the person's accounts with those entities.

42. Indeed, the Social Security Administration warns that the process of replacing a Social Security is a difficult one that creates other types of problems, and that it will not be a complete remedy 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.
>
> 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.[14]

43. 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.

44. **Passport Numbers**—As explained by Aura, a leading identity theft protection service, "[p]assports are among the most widely accepted forms of identification, making them

[14] *Identify Theft and Your Social Security Numbers*, Social Security Admin. (June 2021), https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed September 15, 2025).

prime targets for scammers and fraudsters. If scammers steal your passport number, they can impersonate you, create fake travel documents, or even open bank accounts in your name."[15] Indeed, when combined with other PII, such as a name, address, or picture, a "passport number enables scammers to impersonate you, access your online accounts, or target you in sophisticated scams that lead to identity theft."[16]

45. Moreover, "[u]nlike credit card data or personal Social Security numbers, there are few mechanisms in place to alert consumers that their passport numbers have been stolen and possibly used for fraud" making it difficult to determine if criminals are using a forged or fraudulent passport in an individual's name.[17]

46. Based on the value to cybercriminals of the customer PII in its possession, FFCU knew or should have known the importance of safeguarding the PII entrusted to it and of the foreseeable consequences if its data security systems were breached. FFCU failed, however, to take adequate cyber security measures to prevent the Data Breach from occurring.

FFCU BREACHED ITS DUTY TO PROTECT CUSTOMERS' PRIVATE INFORMATION

47. On or about January 23, 2024, FFCU became aware of a cybersecurity event.[18]

48. After becoming aware of the Data Breach, FFCU launched an investigation into the breach, which lasted until August 2025.[19]

---

[15] Yaniv Masjedi, *What Can Scammers Do With Your Passport Number*?, Aura (Apr. 12, 2023), https://www.aura.com/learn/what-can-someone-do-with-your-passport-number#:~:text=If%20scammers%20steal%20your%20passport,could%20still%20be%20at%20risk.

[16] *Id.*

[17] Kate Fazzini, *Here's how criminals use stolen passport information*, CNBC (July 5, 2019), https://www.cnbc.com/2019/07/05/how-criminals-use-stolen-passport-information.html.

[18] *See* FFCU – 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 September 15, 2025).

[19] *Id.*

49. According to the dark web monitoring service Ransomware Live it appears that now-defunct ransomware cartel BlackBasta targeted Defendant.[20]

50. On or around September 11, 2025, nearly two years after the Data Breach began, FFCU reported the Data Breach to the Office of the Maine Attorney General, indicating the Data Breach compromised the Private Information of 187,038 individuals.[21]

51. As set forth below, despite this threat, and other known threats, upon information and belief, FFCU failed to take any action to increase security of the Private Information it held and knew to be highly valuable to cybercriminals.

52. On or around the time FFCU notified Maine's Attorney General of the Data Breach, Plaintiffs received a notice informing them that their Private Information had been compromised during the Data Breach.

53. Upon information and belief, Class Members received similar notices informing them that their Private Information was compromised during the Data Breach.

54. Further, on Defendant's website, it posted certain, limited information regarding the Data Breach.[22]

***

> On January 23, 2024, FFCU became aware that it had experienced a data security incident. Upon learning of this issue, FFCU immediately commenced a prompt and thorough investigation. As part of the investigation, FFCU engaged external cybersecurity professionals who regularly investigate and analyze these types of situations to help determine the extent of any compromise of the information on the FFCU network and conducted a manual review. After an extensive investigation, we concluded

[20] https://cybernews.com/security/fairmont-federal-credit-union-data/ (last visited September 16, 2025).
[21] *Data Breach Notifications*, Office of the Maine Attorney General, https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/75c92a2c-3791-47c6-84f7-87b34fab952d.html (last visited September 15, 2025).
[22] https://cdn.firstbranchcms.com/kcms-doc/163/91576/FFCU-Website-Substitute-Notice-April-28-2025-35873074.1.pdf (last visited September 16, 2025).

> on or about August 17, 2025 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. Not all data elements were impacted for every individual.
>
> **To date, FFCU is not aware of any incidents of identity theft or financial fraud as a result of the incident.** Nevertheless, out of an abundance of caution, commencing on September 11, 2025, FFCU notified individuals whose information may have been included in the files access by the unauthorized party. Notified individuals have been provided with best practices to protect their information, including placing a Fraud Alert and Security Freeze on their credit files, and obtaining a free credit report. Additionally, you should always remain vigilant in reviewing your financial account statements and credit reports for irregular activity over the next twelve to twenty-four months. If you see charges or activity that you do not recognize, please contact the relevant financial institution immediately. Finally, individuals whose SSN were potentially impacted have been offered complimentary credit monitoring.

***

55. The Data Breach occurred as a direct result of FFCU's failure to implement and follow basic security procedures to protect its current and former customers' Private Information that it had collected and stored.

FFCU FAILED TO COMPLY WITH FTC GUIDELINES

56. FFCU is prohibited by the Federal Trade Commission Act, 15 U.S.C. § 45 ("FTC Act") from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission ("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.

57. 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.[23]

58. Among other guidance, the FTC recommends the following cybersecurity guidelines for businesses in order to protect sensitive information in their systems: [24]

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 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;

[23] *Start with Security – A Guide for Business*, United States Federal Trade Comm'n (2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last accessed September 16, 2025).
[24] *Protecting Personal Information: A Guide for Business*, United States Federal Trade Comm'n, https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last accessed September 16, 2025).

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.

59. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to private 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.[25]

60. 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.

[25] *Id.*

61. FFCU failed to properly implement basic data security practices. FFCU's failure to employ reasonable and appropriate measures to protect against unauthorized access to its customers' PII constitutes an unfair act of practice prohibited by Section 5 of the FTC Act.

62. FFCU was at all times fully aware of its obligations to protect the PII of its customers given the reams of PII that it had access to. FFCU was also aware of the significant repercussions that would result from a failure to properly secure the Private Information it maintained.

FFCU FAILURE TO PREVENT, IDENTIFY, AND TIMELY REPORT THE DATA BREACH

63. FFCU admits that an unauthorized third-party accessed it information technology system.[26]

64. FFCU failed to take necessary precautions or employ adequate measures necessary to protect its computer systems against unauthorized access and keep Plaintiffs and Class Members' Private Information secure.

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

66. Despite its own knowledge of the inherent risks of cyberattacks, and notwithstanding the FTC's data security principles and practices[27], FFCU failed to disclose that its systems and security practices were inadequate to reasonably safeguard individuals' Private Information.

---

[26] https://cdn.firstbranchcms.com/kcms-doc/163/91576/FFCU-Website-Substitute-Notice-April-28-2025-35873074.1.pdf (last visited September 15, 2025).

[27] 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 September 16, 2025).

67. 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.[28] Immediate notification to individuals impacted by a data breach is critical so that those impacted can take measures to protect themselves.

THE DATA BREACH'S INCLUSION OF PHI IS PARTICULARLY SIGNIFICANT

68. With respect to the data breaches implicating PHI, a study found "the majority [70%] of data impacted by healthcare breaches could be leveraged by hackers to commit fraud or identity theft."[29]

69. "Actors buying and selling PII and PHI from healthcare institutions and providers in underground marketplaces is very common and will almost certainly remain so due to this data's utility in a wide variety of malicious activity ranging from identity theft and financial fraud to crafting of bespoke phishing lures."[30]

70. The reality is that cybercriminals seek nefarious outcomes from a data breach and "stolen health data can be used to carry out a variety of crimes."[31]

71. Health information in particular is likely to be used in detrimental ways - by leveraging sensitive personal health details and diagnoses to extort or coerce someone, and serious and long-term identity theft.[32]

72. As indicated by Jim Trainor, second in command at the FBI's cyber security division: "Medical records are a gold mine for criminals - they can access a customer's name,

---

[28] *Id.*
[29] https://distilgovhealth.com/2019/10/03/70-of-data-involved-in-healthcare-breaches-increases-risk-of-fraud/ (last visited September 16, 2025).
[30] *Id.*
[31] https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon (last visited September 16, 2025).
[32] *Id.*

DOB, Social Security and insurance numbers, and even financial information all in one place. Credit cards can be, say, five dollars or more where PHI records can go from $20 say up to - we've even seen $60 or $70."[33]

73. The "high value of medical records on the dark web has surpassed that of social security and credit card numbers. These records can sell for up to $1,000 online . . ."[34]

74. Cybercriminals sell health information at a far higher premium than stand-alone PII. This is because health information enables thieves to go beyond traditional identity theft and obtain medical treatments, purchase prescription drugs, submit false bills to insurance companies, or even undergo surgery under a false identity. The shelf life for this information is also much longer—while individuals can update their credit card numbers, they are less likely to change their health insurance information. When medical identity theft occurs, the associated costs to victims can be exorbitant. According to a 2015 study, at least 65% of medical identity theft victims had to "pay an average of $13,500 to resolve the crime."[35]

75. As noted above, some of the information that was compromised in the Data Breach included, among other things, treatment information/diagnosis, prescription information, provider name, MRN/patient ID, and Medicare/Medicaid number.[36] Accordingly, Plaintiffs and Class

[33] IDExperts, You Got It, They Want It: Criminals Targeting Your Private Healthcare Data, New Ponemon Study Shows: https://www.idexpertscorp.com/knowledge-center/single/you-got-it-they-want-it-criminals-are-targeting-your-private-healthcare-dat (last visited September 16, 2025).
[34] https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon (last visited September 16, 2025).
[35] Justin Klawans, What is medical identity theft and how can you avoid it?, The Week (Aug. 2, 2023), https://theweek.com/feature/briefing/1025328/medical-identity-theft-how-to-avoid.
[36] *See* FFCU – 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 September 15, 2025).

Members must remain especially vigilant given the highly sensitive nature of the PHI at issue in this Data Breach.

FFCU FAILED TO COMPLY WITH HIPPA'S MANDATES

76. Defendant is a covered entity under HIPAA (45 C.F.R. § 160.102) and is 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.

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

78. HIPPA's Standards for Privacy of Individually Identifiable Health Information establishes national standards for the protection of health information, while HIPPA's Security Standards for the Protection of Electronic Protected Health Information establishes national security standards for health information that is stored or transmitted electronically.

79. HIPAA requires "comply[iance] with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronic protected health information." 45 C.F.R. § 164.302. Such health information includes "individually identifiable health information . . . that is (i) transmitted by electronic media; maintained in electronic media." 45 C.F.R. § 160.103.

80. HIPPA's Security Rule requires entities such as FFCU to, *inter alia*, do the following: (i) ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits; (ii)

protect against any reasonably anticipated threats or hazards to the security or integrity of such information; (iii) protect against any reasonably anticipated uses or disclosures of such information that are not permitted; and (iv) ensure compliance by its workforce.

81. HIPAA also requires entities such as FFCU 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, FFCU is required under HIPAA to "[i]implement 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).

82. Moreover, both HIPPA and HITECH required FFCU 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.

83. Finally, HIPPA requires an entity to provide notice of a data breach to affected individuals "without unreasonable delay and in no case later than 60 days following discovery of the breach." 45 C.F.R. §§ 164.400-414.

84. FFCU was, at all times, aware of the mandates of HIPPA. Despite being aware of these mandates and its concomitant obligations, FFCU failed to comply with its obligations and protect the PHI of Plaintiffs and the Class Members.

85. Defendant's failure in this regard is especially egregious given that Defendant was fully aware of the breadth and depth of PHI it obtained and stored and the foreseeable consequences that would result from unauthorized disclosure of this information.

PLAINTIFFS AND CLASS MEMBERS SUFFERED DAMAGES

86. The ramifications of FFCU's failure to keep Private Information secure are long-lasting and severe. Once Private Information is stolen, fraudulent use of that information and damage to victims may continue for years.

87. Once Private Information is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or obtained against future misuse. For this reason, Plaintiffs and Class Members will need to maintain these heightened measures for years, and possibly their entire lives as a result of Defendant's conduct. Further, the value of Plaintiffs' and Class Members' Private Information has been diminished by its exposure in the Data Breach.

88. 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.[37] "Fullz" packages, which includes "extra information about the legitimate credit card owner in case" the scammer's "bona fides are challenged when they attempt to use the credit card" are also offered on the dark web.[38]

89. Plaintiffs and Class Members are at substantial increased risk of suffering identity theft and fraud or misuse of their Private Information as a result of the Data Breach. From a recent study, 28% of individuals affected by a data breach become victims of identity fraud—this is a

[37] Stolen PII & Ramifications: Identity Theft and Fraud on the Dark Web, Armor (Apr. 3, 2018), https://res.armor.com/resources/blog/stolen-pii-ramifications-identity-theft-fraud-dark-web/.

[38] *Id*.

significant increase from a 2012 study that found only 9.5% of those affected by a breach would be subject to identity fraud. Without a data breach, the likelihood of identify fraud is only about 3%.[39]

90. Plaintiff Butler has in fact already suffered from the theft of his PII when twenty-five thousand dollars ($25,000) was fraudulently wired out of his account to a third-party account.

91. Further, Plaintiffs and Class Members have incurred and will incur out of pocket costs for protective measures, such as identity theft protection, credit monitoring, credit report fees, credit freeze fees, and similar costs related to the Data Breach.

92. Plaintiff Butler has already incurred expense and time protecting his information, including filing identity-theft reports, placing fraud alerts/freezes on various accounts and consolidating all correspondence, logs, and supporting records.

93. Besides the monetary damage sustained in the event of identity theft, consumers may have to spend hours trying to resolve identity theft issues. For example, the FTC estimates that it takes consumers an average of 200 hours of work over approximately six months to recover from identity theft.[40]

94. Plaintiffs and Class Members are also at a continued risk because their information remains in FFCU's systems, which the Data Breach showed are susceptible to compromise and attack and are subject to further attack so long as FFCU fails to take necessary and appropriate security and training measures to protect the Private Information in its possession.

---

[39] Stu Sjouwerman, *28 Percent of Data Breaches Lead to Fraud*, KnowBe4, https://blog.knowbe4.com/bid/252486/28-percent-of-data-breaches-lead-to-fraud (last accessed September 16, 2025).

[40] Kathryn Parkman, *How to Report identity Theft*, ConsumerAffairs (Feb. 17, 2022), https://www.consumeraffairs.com/finance/how-to-report-identity-theft.html (last accessed September 16, 2025).

95. Plaintiffs and Class Members have suffered emotional distress as a result of the Data Breach, the increased risk of identity theft and financial fraud, and the unauthorized exposure of their Private Information to strangers.

96. As a result of FFCU's failure to prevent the Data Breach, Plaintiffs and Class Members have suffered and will continue to suffer injuries, including out of pocket expenses; loss of time and productivity through efforts to ameliorate, mitigate, and deal with the future consequences of the Data Breach; theft of their valuable Private Information; the imminent and certainly impeding injury flowing from fraud and identity theft posed by their Private Information being disclosed to unauthorized recipients and cybercriminals; damages to and diminution in value of their Private Information; and continued risk to Plaintiffs' and the Class Members' Private Information, which remains in the possession of Defendant and which is subject to further breaches so long as FFCU fails to undertake appropriate and adequate measures to protect the Private Information entrusted to it.

CLASS ALLEGATIONS

97. Plaintiffs bring this class action on behalf of themselves and all other individuals who are similarly situated pursuant to Rule 23 of the Federal Rules of Civil Procedure.

98. Plaintiffs seek to represent a class of persons to be defined as follows:

> All individuals in the United States whose Private Information was compromised in the Data Breach (the "Class").

99. Excluded from the Class are FFCU, its subsidiaries and affiliates, officers and directors, any entity in which Defendant has a controlling interest, the legal representative, heirs, successors, or assigns of any such excluded party, the judicial officer(s) to whom this action is assigned, and the members of their immediate families.

100. This proposed class definition is based on the information available to Plaintiffs at this time. Plaintiffs may modify the class definition in an amended pleading or when they move for class certification, as necessary to account for any newly learned or changed facts as the situation develops and discovery gets underway.

101. **Numerosity:** Plaintiffs are informed and believes, and thereon alleges, that there are at minimum, tens of thousands of members of the Class described above. The exact size of the Class and the identities of the individual members are identifiable through Defendant's records, including but not limited to the files implicated in the Data Breach, but based on public information, the Class includes at least 187,038 individuals.

102. **Commonality:** This action involved questions of law and fact common to the Class. Such common questions include but are not limited to:

a. Whether Defendant had a duty to protect the Private Information of Plaintiffs and Class Members;

b. Whether Defendant was negligent in collecting and storing Plaintiffs' and Class Members' Private Information, and breached its duties thereby;

c. Whether Plaintiffs and Class Members are entitled to damages as a result of Defendant's wrongful conduct; and

d. Whether Plaintiffs and Class Members are entitled to restitution as a result of Defendant's wrongful conduct.

103. **Typicality:** Plaintiffs' claims are typical of the claims of the members of the Class. The claims of the Plaintiffs and members of the Class are based on the same legal theories and arise from the same unlawful and willful conduct. Plaintiffs and members of the Class were

customers of Defendant and each had their Private Information exposed and/or accessed by an unauthorized third-party.

104. **Adequacy of Representation:** Plaintiffs are adequate representatives of the Class because their interests do not conflict with the interests of the members of the Class. Plaintiffs will fairly, adequately, and vigorously represent and protect the interests of the members of the Class and has no interests antagonistic to the members of the Class. In addition, Plaintiffs have retained counsel who are competent and experienced in the prosecution of class action litigation. The claims of Plaintiffs and the Class Members are substantially identical as explained above.

105. **Superiority:** This class action is appropriate for certification because class proceedings are superior to other available methods for the fair and efficient adjudication of this controversy and joinder of all members of the Class is impracticable. This proposed class action presents fewer management difficulties than individual litigation, and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court. Class treatment will create economies of time, effort, and expense, and promote uniform decision-making.

106. **Predominance:** Common questions of law and fact predominate over any questions affecting only individual Class Members. Similar or identical violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that dominate this action. For example, Defendant's liability and the fact of damages is common to Plaintiffs and each member of the Class. If Defendant breached its duty to Plaintiffs and Class Members, then Plaintiffs and each Class member suffered damages by that conduct.

107. **Injunctive Relief:** Defendant has acted and/or refused to act on grounds that apply generally to the Class, making injunctive and/or declaratory relief appropriate with respect to the Class under Fed. R. Civ. P. 23(b)(2).

108. **Ascertainability:** Members of the Class are ascertainable. Class membership is defined using objective criteria, and Class Members may be readily identified through Defendant's books and records.

CLAIMS FOR RELIEF

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

109. Plaintiffs re-allege the above allegations as if fully set forth herein.

110. Defendant's customers, including Plaintiffs and Class Members, provided their non-public Private Information to Defendant as a condition of obtaining services from Defendant.

111. Defendant owed a duty to Plaintiffs and Class Members to exercise reasonable care in securing, safeguarding, storing, and protecting the PII and PHI it collected from them as a condition of obtaining services from FFCU from being compromised, lost, stolen, accessed and misused by unauthorized parties. This duty includes, among other things, designing, maintaining, overseeing, and testing Defendant's security systems to ensure that PII and PHI in FFCU's possession was adequately secured and protected

112. Defendant had full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiff and Class Members could and would suffer if their Private Information were wrongfully disclosed.

113. Defendant owed a duty of care to Plaintiffs and Class Members to provide reasonable security, consistent with industry standards, to ensure that its systems and networks adequately protected their Private Information.

114. Defendant had a special relationship with Plaintiffs and Class Members. Plaintiffs and Class Members' willingness to entrust FFCU with their Private Information as a condition of obtaining services was predicated on the understanding that FFCU would take adequate security precautions to protect their PII and PHI.

115. By assuming the responsibility to collect and store this data, Defendant had duties of care to use reasonable means to secure and to prevent disclosure of the information, and to safeguard the information from theft.

116. Plaintiffs and members of the Class entrusted Defendant with their PII and PHI with the understanding that FFCU would safeguard their information.

117. Defendant's conduct also created a foreseeable risk of harm to Plaintiffs and Class Members by failing to: (a) secure its systems and exercise adequate oversight of its data security protocols; (b) ensure compliance with industry standard data security practices, (c) implement adequate system and event monitoring, and (d) implement the systems, policies, and procedures necessary to prevent the Data Breach.

118. Defendant knew, or should have known, of the risks inherent in collecting and storing PII and PHI, the vulnerabilities of its systems, and the importance of adequate security. Defendant should have been aware of numerous, well-publicized data breaches in the months and years preceding the Data Breach.

119. Defendant breached its common law duty to act with reasonable care in collecting and storing the Private Information of its customers, which exists independently from any

contractual obligations between the parties. Specifically, Defendant breached its common law, statutory, and other duties to Plaintiffs and Class Members in numerous ways, including by:

a. failing to adopt reasonable data security measures, practices, and protocols;

b. failing to implement data security systems, practices, and protocols sufficient to protect Plaintiffs' and Class Members' PII and PHI;

c. storing former customers' PII and PHI longer than reasonably necessary;

d. failing to comply with industry-standard data security measures; and

e. failing to timely disclose critical information regarding the nature of the Data Breach.

120. Defendant's failure to implement and maintain adequate data security measures to protect Plaintiffs' and Class Members' Private Information created conditions conducive to a foreseeable, intentional criminal act in the form of the Data Breach. Plaintiffs and Class Members did not contribute to the Data Breach or the subsequent misuse of their Private Information.

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

122. Moreover, Defendant had a duty to promptly and adequately notify Plaintiffs and Class Members of the Data Breach.

123. Defendant had and continues to have duties to adequately disclose that the Private Information of Plaintiffs and Class Members within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice is necessary to allow Plaintiffs and Class Members to take steps to prevent,

mitigate, and repair any identity theft and the fraudulent use of their Private Information by third parties.

124. Defendant's conduct was particularly unreasonable given the nature and amount of Private Information it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiffs and Class Members.

125. Defendant has admitted that the Private Information of Plaintiff and Class Members was wrongfully disclosed to unauthorized third persons as a result of the Data Breach.

126. Defendant's conduct was particularly unreasonable given the nature and amount of Private Information it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiffs and Class Members.

127. 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 or failing to use reasonable measures to protect PII and PHI. Various FTC publications and orders also form the basis of Defendant's duty.

128. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect Plaintiff's and Class Members' PII and PHI and not complying with the industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of PII and PHI they obtained and stored and the foreseeable consequences of a data breach involving the PII and PHI they obtained when providing laboratory and pathology services.

129. Plaintiffs and Class Members are within the class of persons that Section 5 of the FTC Act is intended to protect.

130. Moreover, the harm that has occurred is the type of harm that Section 5 of FTC Act was intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against

businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiffs and Class Members.

131. Defendant's violation of Section 5 of the FTC Act constitutes negligence per se.

132. Furthermore, Defendant is Covered Entities under HIPAA, which sets minimum federal standards for privacy and security of PHI. Pursuant to HIPAA, 42 U.S.C. § 1302d, et. seq., and its implementing regulations, Defendant had a duty to implement and maintain reasonable and appropriate administrative, technical, and physical safeguards to protect Plaintiff's and the Class members' electronic PHI.

133. Specifically, HIPAA required Defendant to: (a) ensure the confidentiality, integrity, and availability of all electronic PHI they create, receive, maintain, or transmit; (b) identify and protect against reasonably anticipated threats to the security or integrity of the electronic PHI; (c) protect against reasonably anticipated, impermissible uses, or disclosures of the PHI; and (d) ensure compliance by its workforce to satisfy HIPAA's security requirements. 45 C.F.R. § 164.102, et. seq.

134. HIPAA also requires Defendant to provide Plaintiffs and Class Members with notice of any breach of their individually identifiable PHI "without unreasonable delay and in no case later than 60 calendar days after discovery of the breach." 45 C.F.R. §§ 164.400-414.

135. Defendant violated HIPAA by disclosing Plaintiff's and the Class Members' electronic PHI; by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' PHI; and by failing to provide Plaintiffs and Class Members with notification of the Data Breach without unreasonable delay after its discovery.

136. Plaintiffs and the Class Members are customers within the class of persons HIPAA was intended to protect, as they are customers of Defendant's insurance policies.

137. Moreover, the harm that has occurred is the type of harm that the HIPAA was intended to guard against.

138. Defendant's violation of HIPAA constitutes negligence per se

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

140. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have and will suffer damages including, but not limited to: (a) the loss of value of their Private Information and loss of opportunity to determine for themselves how their PII and PHI is used; (b) the publication and/or theft of their PII and PHI; (c) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII and PHI; (d) lost opportunity costs associated with addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest and recover from tax fraud and identity theft; (e) time, effort, and expense associated with placing fraud alerts or freezes on credit reports; (f) anxiety, emotional distress, loss of privacy, and other economic and non-economic losses; (g) the continued risk to their PII and PHI, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as FFCU fails to undertake appropriate and adequate measures to protect it; and, (h) future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the inevitable and continuing consequences of compromised for the rest of their lives.

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

142. As a direct and proximate result of Defendant's negligence, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (a) invasion of privacy; (b) lost or diminished value of Private Information; (c) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (d) loss of benefit of the bargain; (e) an increase in spam calls, texts, and/or emails; and (f) the continued and certainly increased risk to their Private Information, which: (i) remains unencrypted and available for unauthorized third parties to access and abuse; and (ii) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

143. As a direct and proximate result of Defendant's negligence, Plaintiffs and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

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

further unauthorized disclosures so long as Defendant fail to undertake appropriate and adequate measures to protect the Private Information in its continued possession.

145. Plaintiffs and Class Members are therefore entitled to damages, including restitution and unjust enrichment, declaratory and injunctive relief, and attorneys' fees, costs, and expenses.

COUNT II
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiffs and the Class)

146. Plaintiffs re-allege the above allegations as if fully set forth herein.

147. In connection with obtaining services from Defendant, Plaintiffs and Class Members entered into implied contracts with FFCU.

148. Plaintiffs and Class Members were required to deliver their Private Information to Defendant as part of the process of obtaining services from Defendant.

149. Defendant solicited, offered, and invited Class Members to provide their Private Information in order to obtain services at Defendant's. Plaintiffs and Class Members accepted Defendant's offers and provided their Private Information to Defendant.

150. Defendant accepted possession of Plaintiffs' and Class Members' Private Information for the purpose of providing services to Plaintiffs and Class Members.

151. When Plaintiffs and Class Members provided their PII and PHI to FFCU, either directly or indirectly, as a pre-condition for obtaining services, they entered into implied contracts with FFCU.

152. Pursuant to these implied contracts, in exchange for the consideration and PII and PHI provided by Plaintiffs and Class Members, Defendant agreed to, among other things, and Plaintiffs and Class Members understood that FFCU would: (a) provide products and/or services to Plaintiffs and Class Members; (b) implement reasonable measures to protect the security and

confidentiality of Plaintiff's and Class Members' PII and PHI; and (c) protect Plaintiffs' and Class Members' PII and PHI in compliance with federal and state laws and regulations and industry standards.

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

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

155. The protection of PII and PHI was a material term of the implied contracts between Plaintiffs and Class Members, on the one hand, and Defendant, on the other hand. Indeed, as set forth herein, Defendant recognized its duty to provide adequate data security and ensure the privacy of its customers' PII and PHI with its practice of providing a privacy policy on its website.

156. Plaintiffs and Class Members performed their obligations under the implied contract when they provided Defendant with their PII and PHI.

157. Defendant breached its obligations under its implied contracts with Plaintiffs and Class Members in failing to implement and maintain reasonable security measures to protect and secure their PII and PHI, and in failing to implement and maintain security protocols and

procedures to protect Plaintiffs' and Class Members' PII and PHI in a manner that complies with applicable laws, regulations, and industry standards

158. The mutual understanding and intent of Plaintiffs and Class Members on the one hand, and Defendant, on the other, is demonstrated by their conduct and course of dealing.

159. On information and belief, at all relevant times, Defendant promulgated, adopted, and implemented written privacy policies whereby it expressly promised Plaintiffs and Class Members that it would only disclose Private Information under certain circumstances, none of which relate to the Data Breach.

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

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

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

163. Importantly, West Virginia law provides that every contract includes good faith and fair dealing between the parties involved.

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

165. Defendants breached the implied contracts it made with Plaintiffs and the Class by failing to safeguard and protect their Private Information, by failing to delete the information of

Plaintiffs and the Class once the relationship ended, and by failing to provide accurate notice to them that Private Information was compromised as a result of the Data Breach.

166. Defendant breached the implied covenant of good faith and fair dealing by failing to maintain adequate computer systems and data security practices to safeguard Private Information, failing to timely and accurately disclose the Data Breach to Plaintiffs and Class Members and continued acceptance of Private Information and storage of other personal information after Defendant knew, or should have known, of the security vulnerabilities of the systems that were exploited in the Data Breach.

167. Defendant's breach of its obligations of its implied contracts with Plaintiffs and Class Members directly resulted in the Data Breach and the injuries that Plaintiff and Class Members have suffered from the Data Breach.

168. Plaintiffs and Class Member suffered by virtue of Defendant's breach of their implied contracts because: (a) they paid for data security protection they did not receive; (b) they face a substantially increased risk of identity theft - risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (c) their PII and PHI was improperly disclosed to unauthorized individuals; (d) the confidentiality of their PII and PHI has been breached; (e) they were deprived of the value of their PII and PHI, for which there is a well-established national and international market; (f) they have lost time and incurred expenses, and will incur future costs to mitigate and remediate the effects of the Data Breach, including the increased risks of identity theft they face and will continue to face; and (g) they have overpaid for the services they received without adequate data security.

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

170. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to, *e.g.*, (a) strengthen its data security systems and monitoring procedures; (b) submit to future annual audits of those systems and monitoring procedures; and (c) immediately provide adequate credit monitoring to all Class Members.

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

171. Plaintiffs re-allege the above allegations as if fully set forth herein.

172. This count is plead in the alternative to the breach of implied contract count above.

173. By its wrongful acts and omissions described herein, Defendant has obtained a benefit by unduly taking advantage of Plaintiffs and Class Members.

174. Plaintiffs and Class Members conferred a benefit on Defendant, whereby they provided their Private Information to Defendant to obtain services.

175. Defendant prior to and at the time Plaintiffs and Class Members entrusted it with their PII and PHI, caused Plaintiffs and Class Members to reasonably believe that it would keep that Private Information secure.

176. The monies Defendant was paid in its ordinary course of business included a premium for Defendant's cybersecurity obligations and were supposed to be used by Defendant, in part, to pay for the administrative and other costs of providing reasonable data security and protection for Plaintiffs' and Class Members' Private Information.

177. Defendant knew that Plaintiffs and Class Members conferred a benefit upon it and accepted and retained that benefit by accepting and retaining the Private Information entrusted to it. Defendant profited from Plaintiffs' retained data and used Plaintiffs' and Class Members' Private Information for business purposes.

178. Defendant failed to disclose facts pertaining to its substandard information systems, or defects and vulnerabilities therein before Plaintiffs and Class Members made their decisions to provide Defendant with their Private Information.

179. Defendant enriched itself by hoarding the costs it reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' Private Information. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant calculated to increase its own profit at the expense of Plaintiffs and Class Members by utilizing cheap, ineffective security measures and diverting those funds to its own personal use. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite security and the safety of their Private Information.

180. Defendant failed to provide reasonable security, safeguards, and protections to the Private Information of Plaintiffs and Class Members, and as a result, Defendant was overpaid.

181. Under principles of equity and good conscience, Defendant should not be permitted to retain any of the benefits that Plaintiffs and Class Members conferred upon it.

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

183. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (a) invasion of privacy; (b) lost or diminished value of Private Information; (c) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (d) loss of benefit of the bargain; (e) an increase in spam calls, texts, and/or emails; and (f) the continued and certainly increased risk to their Private Information, which: (i) remains unencrypted and available for unauthorized third parties to access and abuse; and (ii) remains backed up in Defendant's

possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

184. Plaintiffs and Class Members are entitled to full refunds, restitution, and/or damages from Defendant and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Defendant from its wrongful conduct. This can be accomplished by establishing a constructive trust from which Plaintiffs and Class Members may seek restitution or compensation.

COUNT IV
DECLARATORY JUDGMENT
(On Behalf of Plaintiffs and the Class)

185. Plaintiffs re-allege all preceding allegations above as if fully set forth herein.

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

187. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiffs' and Class Members' Private Information and whether FFCU is currently maintaining data security measures adequate to protect Plaintiffs and Class Members from further data breaches that compromise their PII. Plaintiffs allege that FFCU's data security measures remain inadequate. Furthermore, Plaintiffs continue to suffer injury as a result of the compromise of their PII and remains at imminent risk that further compromises of their PII will occur in the future.

188. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. FFCU owes a legal duty to secure customers' Private Information and to timely notify impacted individuals of a data breach under the common law, HIPPA, and various state statutes; and

b. FFCU continues to breach this legal duty by failing to employ reasonable measures to secure Private Information in its possession.

189. This Court also should issue corresponding prospective injunctive relief requiring FFCU to employ adequate security protocols consistent with law and industry standards to protect Private Information in FFCU's data network.

190. If an injunction is not issued, Plaintiffs will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at FFCU. The risk of another such breach is real, immediate, and substantial. If another breach at FFCU occurs, Plaintiffs will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

191. The hardship to Plaintiffs if an injunction is not issued exceeds the hardship to FFCU if an injunction is issued. Plaintiffs will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to FFCU of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and FFCU has a pre-existing legal obligation to employ such measures.

192. Issuance of the requested injunction will not disserve the public interest. In contrast, such an injunction would benefit the public by preventing another data breach at FFCU, thus eliminating the additional injuries that would result to Plaintiffs and customers whose confidential information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs pray for judgment as follows:

A. For an Order certifying this action as a class action, appointing Plaintiffs as class representatives for the Class, and appointing their counsel to represent the Class;

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

C. For equitable relief compelling FFCU to utilize appropriate methods and policies with respect to customer data collection, storage, and safety, and to disclose with specificity the types of PII and PHI compromised as a result of the Data Breach;

D. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of FFCU's wrongful conduct;

E. Ordering FFCU to pay for not less than ten years of credit monitoring services for Plaintiffs and Class Members;

F. For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

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

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

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

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

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury on all claims so triable.

Dated: September 16, 2025

Respectfully submitted,

/s/ Christopher D. Pence

Christopher D. Pence (WVSB # 9095)
Michael W. Taylor (WVSB # 11715)
Pence Law Firm PLLC
10 Hale Street, 4th Floor
Charleston, WV 25329
(304) 345-7250 (Phone)
cpence@pencefirm.com
mtaylor@pencefirm.com

and

LYNCH CARPENTER, LLP
Gerald D. Wells, III (*pro hac vice* forthcoming)
Robert J. Gray (*pro hac vice* forthcoming)
1760 Market Street, Suite 600
Philadelphia, PA 19103
T: 267-609-6910
jerry@lcllp.com
rob@lcllp.com

Attorneys for Plaintiffs 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

Richard Butler and Timothy Knotts

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

(c) Attorneys *(Firm Name, Address, and Telephone Number)*

Chris Pence, Pence Law Firm, 10 Hale Street, 4th Fl
Charleston WV 304-345-7250

DEFENDANTS

Fairmont Federal Credit Union

County of Residence of First Listed Defendant _____
(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)***:
28 USC Section 1332(d)(2)(A)

Brief description of cause:
Action seeking damages for 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
9/16/2025

SIGNATURE OF ATTORNEY OF RECORD
/s/ Christopher D. Pence

FOR OFFICE USE ONLY

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

INSTRUCTIONS FOR ATTORNEYS COMPLETING CIVIL COVER SHEET FORM JS 44

Authority For Civil Cover Sheet

The JS 44 civil cover sheet and the information contained herein neither replaces nor supplements the filings and service of pleading 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. Consequently, a civil cover sheet is submitted to the Clerk of Court for each civil complaint filed. The attorney filing a case should complete the form as follows:

I.(a) **Plaintiffs-Defendants.** Enter names (last, first, middle initial) of plaintiff and defendant. If the plaintiff or defendant is a government agency, use only the full name or standard abbreviations. If the plaintiff or defendant is an official within a government agency, identify first the agency and then the official, giving both name and title.

(b) **County of Residence.** For each civil case filed, except U.S. plaintiff cases, enter the name of the county where the first listed plaintiff resides at the time of filing. In U.S. plaintiff cases, enter the name of the county in which the first listed defendant resides at the time of filing. (NOTE: In land condemnation cases, the county of residence of the "defendant" is the location of the tract of land involved.)

(c) **Attorneys.** Enter the firm name, address, telephone number, and attorney of record. If there are several attorneys, list them on an attachment, noting in this section "(see attachment)".

II. **Jurisdiction.** The basis of jurisdiction is set forth under Rule 8(a), F.R.Cv.P., which requires that jurisdictions be shown in pleadings. Place an "X" in one of the boxes. If there is more than one basis of jurisdiction, precedence is given in the order shown below.
United States plaintiff. (1) Jurisdiction based on 28 U.S.C. 1345 and 1348. Suits by agencies and officers of the United States are included here.
United States defendant. (2) When the plaintiff is suing the United States, its officers or agencies, place an "X" in this box.
Federal question. (3) This refers to suits under 28 U.S.C. 1331, where jurisdiction arises under the Constitution of the United States, an amendment to the Constitution, an act of Congress or a treaty of the United States. In cases where the U.S. is a party, the U.S. plaintiff or defendant code takes precedence, and box 1 or 2 should be marked.
Diversity of citizenship. (4) This refers to suits under 28 U.S.C. 1332, where parties are citizens of different states. When Box 4 is checked, the citizenship of the different parties must be checked. (See Section III below**; NOTE: federal question actions take precedence over diversity cases.**)

III. **Residence (citizenship) of Principal Parties.** This section of the JS 44 is to be completed if diversity of citizenship was indicated above. Mark this section for each principal party.

IV. **Nature of Suit.** Place an "X" in the appropriate box. If there are multiple nature of suit codes associated with the case, pick the nature of suit code that is most applicable. Click here for: Nature of Suit Code Descriptions.

V. **Origin.** Place an "X" in one of the seven boxes.
Original Proceedings. (1) Cases which originate in the United States district courts.
Removed from State Court. (2) Proceedings initiated in state courts may be removed to the district courts under Title 28 U.S.C., Section 1441.
Remanded from Appellate Court. (3) Check this box for cases remanded to the district court for further action. Use the date of remand as the filing date.
Reinstated or Reopened. (4) Check this box for cases reinstated or reopened in the district court. Use the reopening date as the filing date.
Transferred from Another District. (5) For cases transferred under Title 28 U.S.C. Section 1404(a). Do not use this for within district transfers or multidistrict litigation transfers.
Multidistrict Litigation – Transfer. (6) Check this box when a multidistrict case is transferred into the district under authority of Title 28 U.S.C. Section 1407.
Multidistrict Litigation – Direct File. (8) Check this box when a multidistrict case is filed in the same district as the Master MDL docket.
PLEASE NOTE THAT THERE IS NOT AN ORIGIN CODE 7. Origin Code 7 was used for historical records and is no longer relevant due to changes in statute.

VI. **Cause of Action.** Report the civil statute directly related to the cause of action and give a brief description of the cause. **Do not cite jurisdictional statutes unless diversity.** Example: U.S. Civil Statute: 47 USC 553 Brief Description: Unauthorized reception of cable service.

VII. **Requested in Complaint.** Class Action. Place an "X" in this box if you are filing a class action under Rule 23, F.R.Cv.P.
Demand. In this space enter the actual dollar amount being demanded or indicate other demand, such as a preliminary injunction.
Jury Demand. Check the appropriate box to indicate whether or not a jury is being demanded.

VIII. **Related Cases.** This section of the JS 44 is used to reference related cases, if any. If there are related cases, insert the docket numbers and the corresponding judge names for such cases.

Date and Attorney Signature. Date and sign the civil cover sheet.