UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF TEXAS
WICHITA FALLS DIVISION

SUSAN SCOTT and JULIAN CERNA, individually, and on behalf of all others similarly situated,	)	No. 7:25-cv-00052
Plaintiffs,	)	**CLASS ACTION COMPLAINT**
v.	)	**DEMAND FOR JURY TRIAL**
AMERICAN NATIONAL BANK & TRUST,	)	
Defendant.	)	

CLASS ACTION COMPLAINT AND JURY DEMAND

Susan Scott and Julian Cerna ("Plaintiffs"), through their attorneys, individually and on behalf of all others similarly situated, bring this Class Action Complaint against American National Bank & Trust, ("ANBT" or "Defendant"), alleging as follows, based upon information and belief, investigation of counsel, and personal knowledge of Plaintiffs.

INTRODUCTION

1. This class action arises from Defendant's failure to protect highly sensitive data.

2. ANBT lost control over its computer network and cybercriminals accessed highly sensitive personal information of at least 52,977 Texans[1] and citizens' of other states, including at least full names, Social Security numbers, and financial account information ("the Data Breach").

3. Upon information and belief, cybercriminals were able to breach Defendant's systems in January 2025 for several days because Defendant failed to adequately train its

[1] https://oag.my.site.com/datasecuritybreachreport/apex/DataSecurityReportsPage (last viewed May 30, 2025).

employees on cybersecurity, failed to adequately monitor its agents, contractors, vendors, and suppliers in handling and securing the PII of Plaintiffs, and failed to maintain reasonable security safeguards or protocols to protect the Class's PII/PH—rendering it an easy target for cybercriminals.

4. Despite the fact ANBT knew sensitive data had been stolen, ANBT waited until May 2025—approximately 5 months after the Data Breach—before it finally announced the Data Breach to the Texas Attorney General began notifying Class Members about the Data Breach.

5. However, ANBT failed to post a Notice on its website, which is a common industry-standard practice, and provided no public details about the breach, aside from the information it reported to the Texas attorney general (number of Texans affected and types of information affected).

6. ANBT failed to disclose the nature of the Data Breach and the threat it posed, how the Data Breach happened, or why it took approximately 5 months before ANBT finally began notifying some victims that cybercriminals had gained access to their highly private information.

7. Defendant's deliberate failure to timely report the Data Breach made the victims vulnerable to identity theft without any warnings to monitor their financial accounts or credit reports to prevent unauthorized use of their PII.

8. Defendant knew or should have known that each victim of the Data Breach deserved prompt and efficient notice of the Data Breach and assistance in mitigating the effects of PII misuse.

9. In failing to adequately protect its former and current employees' and clients' information, adequately notify them about the breach, and by obfuscating the nature of the breach,

Defendant violated state law and harmed an unknown number of its current and former employees and clients.

10. Plaintiffs and the Class are victims of Defendant's negligence and inadequate cyber security measures. Specifically, Plaintiffs and members of the proposed Class trusted Defendant with their PII. But Defendant betrayed that trust when Defendant failed to properly use up-to-date security practices to prevent the Data Breach.

11. Plaintiffs are victims of the Data Breach. Based on Defendant's notice letter, Plaintiffs' names, Social Security numbers, and financial account information were exposed during the Data Breach.

12. The exposure of one's PII to cybercriminals is a bell that cannot be unrung. Before the Data Breach, the private information of Plaintiffs and the Class were exactly that—private. Not anymore. Now, their private information is permanently exposed and unsecure.

13. Plaintiffs seek on behalf of themselves and the Class, monetary damages and injunctive relief including lifetime credit monitoring and ID theft monitoring.

PARTIES

14. Plaintiff Susan Scott is a natural person and citizen of Iowa Park, Texas, where she intends to remain.

15. Plaintiff Julian Cerna is a natural person and citizen of Wichita Falls, Texas, where she intends to remain.

16. Defendant American National Bank & Trust is a bank incorporated in Texas, with its principal place of business at 2732 Midwestern Parkway, Wichita Falls, TX 76308. It may be served via its registered agent, Roy T. Olsen, at 2732 Midwestern Parkway, Wichita Falls, TX 76308.

JURISDICTION AND VENUE

17. This Court has subject matter 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. Members of the proposed class and Defendant are citizens of different states, as Defendant has notified individuals of the data breach in other states.[2] Additionally, there are over 100 putative Class Members. [3]

18. This Court has personal jurisdiction over Defendant because it is headquartered in Texas, regularly conducts business in Texas, and has sufficient minimum contacts in Texas.

19. Venue is proper in this Court because Defendant's principal office is in this District, and because a substantial part of the events, acts, and omissions giving rise to Plaintiffs' claims occurred in this District.

BACKGROUND

Defendant Collected and Stored the PII of Plaintiffs and the Class

20. ANBT is an independent, locally-owned bank ranked as "the largest, independently owned financial institution…with more than $2.1 billion in assets and [employes] more than 300" in customer service to assist its customers.[4]

21. ANBT accumulates highly personally identifiable information (PII or Private Information) of its former and current customers in order to provide financial services.

22. In collecting and maintaining its customers' PII, ANBT agreed it would safeguard the data in accordance with state law and federal law. After all, Plaintiffs and Class Members themselves took reasonable steps to secure their PII.

---

[2] https://oag.ca.gov/ecrime/databreach/reports/sb24-603161 (last viewed May 30, 2025).
[3] https://oag.my.site.com/datasecuritybreachreport/apex/DataSecurityReportsPage (last viewed May 30, 2025).
[4] https://www.amnat.com/about/(last viewed May 30, 2025).

23. ANBT understood the need to protect its former and current customers PII and prioritize its data security.

24. ANBT emphasizes the importance of safety on its website, It follows that secure and reliable data storage should be deeply important to ANBT.

25. Despite recognizing its duty to do so, on information and belief, ANBT has not implemented reasonable cybersecurity safeguards or policies to protect the PII of its current and former customers, nor trained its IT or data security employees to prevent, detect, and stop breaches of its systems. As a result, ANBT leaves significant vulnerabilities in its systems for cybercriminals to exploit and gain access to the highly valuable Private Information it stored.

Texas Breach Notice Statutes

26. The State of Texas requires that any "person who conducts business in this state and owns or licenses computerized data that includes sensitive personal information shall disclose any breach of system security, after discovering or receiving notification of the breach, to any individual whose sensitive personal information was, or is reasonably believed to have been, acquired by an unauthorized person." Tex. Bus. & Com. Code Ann. § 521.053(b). In fact, "breach of a security system" is defined as "[the] unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of sensitive personal information." Tex. Bus. & Com. Code Ann. § 521.053(a).

27. Because Defendant issued the data breach notification disclosure as required by Tex. Bus. & Com. Code. Ann. § 521.053, following the investigation, Defendant must have concluded that Plaintiff's and Class Members' "sensitive personal information was, or is reasonably believed to have been acquired by an unauthorized person." Tex. Bus. & Com. Code Ann. § 521.053. And this is consistent with the language in the notice letter that the data was not

only accessed but also acquired –i.e., "copied" by the threat actors.

Defendant Failed to Safeguard the PII of Plaintiffs and the Class

28. Plaintiffs are both customers of ANBT.

29. Plaintiffs received Defendant's Notice on or around April 21, 2025, informing them that his PII was compromised.

30. Plaintiffs were shocked to have received this notice because they reasonably believed their Private Information would be protected by a financial institution like ANBT.

31. On information and belief, Defendant collects and maintains its current and former customers' unencrypted PII in its computer systems.

32. In collecting and maintaining PII, Defendant implicitly agreed that it will safeguard the data using reasonable means according to state and federal law.

33. In January 2025, for an unknown length of time, cybercriminals hacked Defendant's network and accessed extremely sensitive information, including social security numbers and financial account information.

34. It is unclear when Defendant discovered the Data Breach. Defendant has only publicly disclosed how many Texans were impacted, and the types of information impacted.[5]

35. Regardless of how long it took Defendant to discover the Data Breach, Defendant's cyber and data security systems were completely inadequate and allowed cybercriminals to obtain files containing a treasure trove of thousands of its employees' and clients' highly private information continuously over an unknown period of time.

36. In May 2025–approximately five months after the Data Breach—Defendant finally began notifying some Class Members the Data Breach.

---

[5] *Data Security Breach Reports – American National Bank & Trust.,* KEN PAXTON ATTORNEY GENERAL OF TEXAS, https://oag.my.site.com/datasecuritybreachreport/apex/DataSecurityReportsPage (last visited May 30, 2025).

37. Thus, Defendant kept the Class in the dark—thereby depriving the Class of the opportunity to try and mitigate their injuries in a timely manner.

38. Despite its duties to safeguard PII, Defendant did not in fact follow industry standard practices in securing current customers' PII, as evidenced by the Data Breach.

39. Defendant has not disclosed what additional controls it has implemented, if any, to improve its security in response to the Data Breach.

40. The risk of identity theft and unauthorized use of Plaintiffs' and Class Members' PII is substantially high given that the data stolen includes Social Security numbers. The fraudulent activity resulting from the Data Breach may not come to light for years.

41. Cybercriminals need not harvest a person's Social Security number or financial account information in order to commit identity fraud or misuse Plaintiffs' and the Class's PII (although in Plaintiffs' case, his Social Security number was compromised). Cybercriminals can cross-reference the data stolen from the Data Breach and combine with other sources to create "Fullz" packages, which can then be used to commit fraudulent account activity on Plaintiffs and the Class's financial accounts.

42. On information and belief, Defendant failed to adequately train its IT and data security patients on reasonable cybersecurity protocols or implement reasonable security measures, causing it to lose control over its employees' and clients' PII. Defendant's negligence is evidenced by its failure to prevent the Data Breach, and to stop cybercriminals from accessing the PII it stored in its network.

43. Furthermore, Defendant obfuscates the nature of the breach, failing to clearly inform the public when Defendant discovered the breach, how it happened, whether Defendant paid a ransom to retrieve the stolen data back, and why it took five months for Defendant to start

notifying victims.

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

44. It is well known that PII, including Social Security numbers, is an invaluable commodity and a frequent target of hackers.

45. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in recent years.

46. In 2024, a 3,158 data breaches occurred, exposing approximately 1,350,835,988 sensitive records—a 211% increase year-over-year.[6]

47. 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. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive to ransomware criminals . . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[7]

48. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in the financial services industry, including Defendant.

49. Despite the prevalence of public announcements of data breach and data security compromises, and despite its own acknowledgments of data security compromises, and despite its own acknowledgment of its duties to keep PII private and secure, Defendant failed to take appropriate steps to protect the PII of Plaintiffs and Class Members from being compromised.

---

[6] *2024 Data Breach Annual Report*, IDENTITY THEFT RESOURCE CENTER, https://www.idtheftcenter.org/publication/2024-data-breach-report/ (last visited April 24, 2025).

[7] 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 April 24, 2025).

50. 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.

51. 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 Plaintiffs' and Class Members' PII 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.

Plaintiffs' Experience and Injuries

52. Plaintiffs are current customers of ANBT. In order to receive financial services from ANBT, Plaintiffs were required to provide their PII, including their name and Social Security Number and were provided with their financial account information.

53. Plaintiffs provided their PII to Defendant and trusted that the company would use reasonable measures to protect it according to state and federal law.

54. As a result of its inadequate cybersecurity measures, Defendant exposed Plaintiffs' PII for theft by cybercriminals and sale on the dark web.

55. Indeed, given the Notice Plaintiffs has received, Plaintiffs' PII has already been published before they were even made aware of the incident or will be published imminently by cybercriminals for further theft and sale on the Dark Web.

56. Plaintiffs do not recall ever learning that their PII was compromised in former a data breach incident, other than the breach at issue in this case.

57. Defendant deprived Plaintiffs of the earliest opportunity to guard themselves against the Data Breach's effects by failing to promptly notify them about the Data Breach.

58. Plaintiffs suffered actual injury from the exposure of their PII —which violates their rights to privacy.

59. Plaintiffs suffered actual injury in the form of damages to and diminution in the value of their PII. After all, PII is a form of intangible property—property that Defendant was required to adequately protect.

60. As a result of the Data Breach, Plaintiffs have each 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 their credit information.

61. Plaintiffs will continue to spend considerable time and effort monitoring their accounts to protect themselves from identity theft. Plaintiffs fear for their personal financial security and uncertainty over what PII was exposed. Plaintiffs have and are experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach. Plaintiffs are experiencing anxiety, distress, and fear regarding how the exposure and loss of their Social Security number will impact them. 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.

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

63. Following the Data Breach, Plaintiffs have experienced a substantial increase in scam and spam text messages and emails, some of which indicate exposure of their financial information.

64. Once an individual's PII is for sale and access on the Dark Web, cybercriminals are able to use the stolen and compromised to gather and steal even more information.[8] On information and belief, Plaintiffs' name, Social Security number, and financial information were compromised as a result of the Data Breach.

65. Plaintiffs have a continuing interest in ensuring that their PII, which, upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiffs and the Proposed Class Face Significant Risk of Continued Identity Theft

66. Plaintiffs and members of the proposed Class have suffered injury from the misuse of their PII that can be directly traced to Defendant.

67. As a result of Defendant's failure to prevent the Data Breach, Plaintiffs and the proposed Class have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. Plaintiffs and the class have suffered or are at an increased risk of suffering:

a. The loss of the opportunity to control how their PII is used;

b. The diminution in value of their PII;

c. The compromise and continuing publication of their PII;

d. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

[8] *What do Hackers do with Stolen Information,* AURA, https://www.aura.com/learn/what-do-hackers-do-with-stolen-information (last visited April 24, 2025).

e. Lost opportunity costs and lost wages associated with the time and effort expended 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 identity theft and fraud;

f. Delay in receipt of tax refund monies;

g. Unauthorized use of stolen PII; and

h. The continued risk to their PII, which remains in the possession of Defendant and is subject to further breaches so long as Defendant fails to undertake the appropriate measures to protect the PII in its possession.

68. Stolen PII is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PII can be worth up to $1,000.00 depending on the type of information obtained.

69. The value of Plaintiffs' and the proposed Class's PII on the black market is considerable. Stolen PII trades on the black market for years, and criminals frequently post stolen private information openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee of course.

70. Social Security numbers are particularly attractive targets for hackers because they can easily be used to perpetrate identity theft and other highly profitable types of fraud. Moreover, Social Security numbers are difficult to replace, as victims are unable to obtain a new number until the damage is done.

71. It can take victims years to spot identity or PII theft, giving criminals plenty of time to use that information for cash.

72. One such example of criminals using PII for profit is the development of "Fullz" packages.

73. Cyber-criminals can cross-reference two sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

74. The development of "Fullz" packages means that stolen PII from the Data Breach can easily be used to link and identify it to Plaintiffs' and the Class's phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII 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 operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiffs and the Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiffs' and members of the Class's stolen PII is being misused, and that such misuse is fairly traceable to the Data Breach.

75. Defendant disclosed the PII of Plaintiffs and members of the proposed Class for criminals to use in the conduct of criminal activity. Specifically, Defendant opened up, disclosed, and exposed the PII of Plaintiffs and the Class to people engaged in disruptive and unlawful business practices and tactics, including online account hacking, extortion, and exposure of stolen PII.

76. Defendant's failure to properly notify Plaintiffs and the Class of the Data Breach exacerbated Plaintiffs' and the Class's injuries by depriving them of the earliest opportunity to

take appropriate measures to protect their PII and take other necessary steps to mitigate the harm caused by the Data Breach.

Consumers Prioritize Data Security

77. In 2024, the technology and communications conglomerate Cisco published the results of its multi-year "Consumer Privacy Survey."[9] Therein, Cisco reported the following:

a. "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."[10]

b. "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."[11]

c. 89% of consumers stated that "I care about data privacy."[12]

d. 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.[13]

e. 51% of consumers revealed that "I have switched companies or providers over their data policies or data-sharing practices."[14]

---

[9] *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 March 19, 2025).
[10] *Id*. at 3.
[11] *Id*.
[12] *Id*. at 9.
[13] *Id*.
[14] *Id*.

f. 75% of consumers stated that "I will not purchase from organizations I don't trust with my data."[15]

Defendant Failed to Adhere to FTC Guidelines

78. 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 PII.

79. 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:

a. protect the personal customer information that they keep;

b. properly dispose of personal information that is no longer needed;

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

80. 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.

81. 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.

---

[15] *Id*. at 11.

82. 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.

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

Defendant Failed to Follow Industry Standards

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

85. 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.

86. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 2.0 (including without limitation PR.AA-01, PR.AA.-02, PR.AA-03, PR.AA-04, PR.AA-05, PR.AT-01, PR.DS-01, PR-DS-02,

PR.DS-10, PR.PS-01, PR.PS-02, PR.PS-05, PR.IR-01, DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09, and RS.CO-04), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

87. 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.

CLASS ACTION ALLEGATIONS

88. Plaintiffs bring this class action under Fed. R. Civ. P. 23(a), 23(b)(2), and 23(b)(3), individually and on behalf of all members of the following class:

> All individuals residing in the United States whose PII was compromised in the Data Breach of ANBT in January 2025, including all those individuals who received notice of the breach.

89. Excluded from the Class are Defendant, its agents, affiliates, parents, subsidiaries, any entity in which Defendant has a controlling interest, any Defendant officer or director, any successor or assign, and any Judge who adjudicates this case, including its staff and immediate family.

90. Plaintiffs reserves the right to amend the class definition.

91. Certification of Plaintiffs' claims for class-wide treatment is appropriate because Plaintiffs can prove the elements of his claims on class-wide basis using the same evidence as would be used to prove those elements in individual actions asserting the same claims.

92. This action satisfies the numerosity, commonality, typicality, and adequacy requirements.

93. **Numerosity.** The Class members are so numerous that joinder of all Class Members is impracticable. Based on Defendant's report to the Texas Attorney General,[16] at least 52,977 Texas are involved in this breach, as well as additional customers living in California and Vermont.[17]

94. **Commonality and Predominance.** Plaintiffs' and the Class Members' claims raise predominantly common fact and legal questions—which predominate over any questions affecting individual Class Members—for which a class wide proceeding can answer for all Class Members. In fact, a class wide proceeding is necessary to answer the following questions:

a. if Defendant had a duty to use reasonable care in safeguarding Plaintiffs' and the Class's PII;

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

c. if Defendant was negligent in maintaining, protecting, and securing PII;

d. if Defendant breached contract promises to safeguard Plaintiffs and the Class's PII;

e. if Defendant took reasonable measures to determine the extent of the Data Breach after discovering it;

f. if Defendant's Breach Notice was reasonable;

g. if the Data Breach caused Plaintiffs and the Class injuries;

[16] https://oag.my.site.com/datasecuritybreachreport/apex/DataSecurityReportsPage (*last viewed* May 30, 2025).
[17] https://ago.vermont.gov/document/2025-05-23-american-national-bank-trust-data-breach-notice-consumers (*last viewed* May 30, 2025).

h. what the proper damages measure is; and

i. if Plaintiffs and the Class are entitled to damages, treble damages, and or injunctive relief.

95. **Typicality.** Plaintiffs' claims are typical of Class Members' claims as each arises from the same Data Breach, the same alleged violations by Defendant, and the same unreasonable manner of notifying individuals about the Data Breach.

96. **Adequacy.** Plaintiffs will fairly and adequately protect the proposed Class's common interests. His interests do not conflict with Class Members' interests. And Plaintiffs have retained counsel—including lead counsel—that is experienced in complex class action litigation and data privacy to prosecute this action on the Class's behalf.

97. **Appropriateness.** The likelihood that individual Class Members will prosecute separate actions is remote due to the time and expense necessary to prosecute an individual case. Plaintiffs is not aware of any litigation concerning this controversy already commenced by others who meet the criteria for class membership described above.

98. **Ascertainability.** All members of the proposed Class are readily ascertainable from information in Defendant's custody and control. After all, Defendant already identified some victims and sent them data breach notices.

FIRST CAUSE OF ACTION
Negligence
(On Behalf of Plaintiffs and the Class)

99. Plaintiffs and the Class repeat and re-allege each and every allegation in the Complaint as if fully set forth herein.

100. Defendant required Plaintiffs and Class Members to submit non-public personal information in order to obtain financial services.

101. Defendant owed a duty of care to secure and safeguard the computer systems holding Plaintiffs' and Class Members' Private Information that Defendant's acquired through their collective actions.

102. The duty included obligations to take reasonable steps to prevent disclosure of the Private Information, and to safeguard the information from theft. Defendant's duties included the responsibility to design, implement, and monitor data security systems, policies, and processes to protect against reasonably foreseeable data breaches such as this Data Breach.

103. 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 Defendant's systems and networks, policies, and procedures, and the personnel responsible for them, adequately protected the Private Information.

104. Defendant each owed a duty of care to safeguard the Private Information due to the foreseeable risk of a data breach and the severe consequences that would result from its failure to so safeguard the Private Information.

105. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and its patients, which is recognized by laws and regulations including but not limited to the FTC Act and Tex. Bus. & Com. Code Ann. § 521.052, as well as common law. Defendant were in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a data breach.

106. In addition, Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

107. Defendant also had a duty under Tex. Bus. & Com. Code Ann. § 521.052(a) "to implement and maintain reasonable procedures, including taking any appropriate corrective action, to protect from unlawful use or disclosure any sensitive personal information collected or maintained by [Defendant] in the regular course of business."

108. Defendant also had a duty under Tex. Bus. & Com. Code Ann. § 521.052(b) to destroy any Private Information that was no longer necessary for it to maintain.

109. 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 are each bound by industry standards to protect confidential Private Information that they either acquire, maintain or store.

110. Defendant breached these duties, and thus were negligent, by failing to use reasonable measures to protect Plaintiffs' and Class Members' Private Information, as alleged and discussed above.

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

112. It was therefore foreseeable that the failure to adequately safeguard Class Members' Private Information would result in one or more types of injuries to Class Members.

113. The imposition of a duty of care on Defendant to safeguard the Private Information they maintained is appropriate because any social utility of Defendant's conduct is outweighed by the injuries suffered by Plaintiffs and Class Members as a result of the Data Breach.

114. As a direct and proximate result of Defendant's negligence, Plaintiffs and Class Members are at a current and ongoing risk of identity theft, and Plaintiffs and Class Members sustained compensatory damages including: (a) invasion of privacy; (b) financial "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (c) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (d) financial "out of pocket" costs incurred due to actual identity theft; (e) loss of time incurred due to actual identity theft; (f) loss of time due to increased spam and targeted marketing emails; (g) diminution of value of their PII; (h) future costs of identity theft monitoring; (i) anxiety, annoyance and nuisance, and (j) the continued risk to their PII, which remains in the possession of Defendant, and which is subject to further breaches, so long as Defendant fail to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' Private Information.

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

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

117. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

SECOND CAUSE OF ACTION
Negligence *per se*
(On Behalf of Plaintiffs and the Class)

118. Plaintiffs and the Class repeat and re-allege each and every allegation in the Complaint as if fully set forth herein.

119. Pursuant to Federal Trade Commission, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Private Information.

120. Defendant had a duty under Tex. Bus. & Com. Code Ann. § 521.052(a) "to implement and maintain reasonable procedures, including taking any appropriate corrective action, to protect from unlawful use or disclosure any sensitive personal information collected or maintained by [Defendant] in the regular course of business."

121. Defendant also had a duty under Tex. Bus. & Com. Code Ann. § 521.052(b) to destroy any Private Information that was no longer necessary for it to maintain.

122. Defendant breached their duties to Plaintiffs and Class Members under the FTC Act and Tex. Bus. & Com. Code Ann. § 521.052, et seq by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Private Information.

123. Defendant's failure to comply with applicable laws and regulations constitutes negligence per se.

124. But for Defendant's wrongful and negligent breach of their duties owed to Plaintiffs and Class Members, Plaintiffs and Class Members would not have been injured.

125. The injury and harm suffered by Plaintiffs and Class Members were the reasonably foreseeable result of Defendant's breach of their duties. Defendant knew or should have known that it was failing to meet its duties, and that Defendant's breach would cause Plaintiffs and Class Members to experience the foreseeable harms associated with the exposure of their Private Information.

126. As a direct and proximate result of Defendant's negligence, Plaintiffs and Class Members are at a current and ongoing risk of identity theft, and Plaintiffs and Class Members sustained compensatory damages including: (a) invasion of privacy; (b) financial "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (c) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (d) financial "out of pocket" costs incurred due to actual identity theft; (e) loss of time incurred due to actual identity theft; (f) loss of time due to increased spam and targeted marketing emails; (g) diminution of value of their PII; (h) future costs of identity theft monitoring; (i) anxiety, annoyance and nuisance, and (j) the continued risk to their PII, which remains in the possession of Defendant, and which is subject to further breaches, so long as Defendant fail to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' Private Information.

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

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

THIRD CAUSE OF ACTION
Breach of Implied Contract
(On Behalf of Plaintiffs and the Class)

129. Plaintiffs incorporate all previous paragraphs as if fully set forth herein.

130. Defendant offered to provide employment and/or services to Plaintiffs and members of the Class if, and in exchange, Plaintiffs and members of the Class provided Defendant with their PII.

131. In turn, Defendant agreed it would not disclose the PII it collects to unauthorized persons.

132. Plaintiffs and the members of the Class accepted Defendant's offer by providing PII to Defendant in exchange for Defendant's services.

133. Implicit in the parties' agreement was that Defendant would provide Plaintiffs and members of the Class with prompt and adequate notice of all unauthorized access and/or theft of their PII.

134. Plaintiffs and the members of the Class would not have entrusted their PII to Defendant in the absence of such an agreement with Defendant.

135. Defendant materially breached the contracts it had entered with Plaintiffs and members of the Class by failing to safeguard such information and failing to notify them promptly of the intrusions into its computer systems that compromised such information. Defendant also breached the implied contracts with Plaintiffs and members of the Class by:

a. Failing to properly safeguard and protect Plaintiffs' and members of the Class's PII;

b. Failing to comply with industry standards as well as legal obligations that are necessarily incorporated into the parties' agreement; and

c. Failing to ensure the confidentiality and integrity of electronic PII that Defendant created, received, maintained, and transmitted.

136. The damages sustained by Plaintiffs and members of the Class as described above were the direct and proximate result of Defendant's material breaches of its agreement(s).

137. Plaintiffs and members of the Class have performed under the relevant agreements, or such performance was waived by the conduct of Defendant.

138. The covenant of good faith and fair dealing is an element of every contract. All such contracts impose upon each party a duty of good faith and fair dealing. The parties must act with honesty in fact in the conduct or transactions concerned. Good faith and fair dealing, in connection with executing contracts and discharging performance and other duties according to their terms, means preserving the spirit—not merely the letter—of the bargain. Put differently, the parties to a contract are mutually obligated to comply with the substance of their contract in addition to its form.

139. Subterfuge and evasion violate the obligation of good faith in performance even when an actor believes their conduct to be justified. Bad faith may be overt or may consist of inaction, and fair dealing may require more than honesty.

140. Defendant failed to advise Plaintiffs and members of the Class of that there was not one but two Data Breach and failed to send Notice to the victims promptly and sufficiently.

141. In these and other ways, Defendant violated its duty of good faith and fair dealing.

142. Plaintiffs and members of the Class have sustained damages because of Defendant's breaches of its agreement, including breaches of it through violations of the covenant of good faith and fair dealing.

143. Plaintiffs and the Class seek compensatory damages for breach of implied contract, which includes the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest, and costs.

FOURTH CAUSE OF ACTION
Unjust Enrichment
(On Behalf of Plaintiffs and the Class)

144. Plaintiffs incorporate all previous paragraphs as if fully set forth herein.

145. Upon information and belief, Defendant funds its data security measures from its

general revenue, including payments made by or on behalf of Plaintiffs and the Class Members.

146. As such, a portion of the payments made by or on behalf of Plaintiffs and the Class Members is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Defendant.

147. Plaintiffs and Class Members conferred a monetary benefit on Defendant. Specifically, they either provided services, in the form of employment, or purchased services from Defendant and/or its agents and in so doing provided Defendant or its agents with their PII. In exchange, Plaintiffs and Class Members should have received from Defendant the goods and services that were the subject of the transaction and have their PII protected with adequate data security.

148. Defendant knew that Plaintiffs and Class Members conferred a benefit which Defendant accepted. Defendant profited from these transactions and used the PII of Plaintiffs and Class Members for business purposes.

149. Plaintiffs and Class Members conferred a monetary benefit on Defendant, by paying Defendant as part of Defendant rendering services, a portion of which was to have been used for data security measures to secure Plaintiffs' and Class Members' PII, and by providing Defendant with their valuable PII.

150. Defendant was enriched by saving the costs it reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' PII. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant calculated to avoid the data security obligations at the expense of Plaintiffs and the Class by utilizing cheaper, ineffective security measures. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

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

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

153. If Plaintiffs and Class Members knew that Defendant had not secured their PII, they would not have agreed to provide their PII to Defendant either directly or through their own financial institutions.

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

155. 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: (i) the loss of the opportunity how their PII is used; (ii) the compromise, publication, and/or theft of their PII; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII; (iv) lost opportunity costs associated with effort expended and the loss of productivity 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 identity theft; (vi) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect PII in their continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and the Class.

156. As a direct and proximate result of Defendant's conduct, Plaintiffs and the Class have suffered and will continue to suffer other forms of injury and/or harm.

157. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class Members, proceeds that it unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiffs and Class Members overpaid for Defendant's services.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of all others similarly situated, prays for relief as follows:

a. For an order certifying the Class, and naming Plaintiffs as representatives of the Class, and Plaintiffs' attorneys as Class Counsel;

b. For an order finding in favor of Plaintiffs and the Class on all counts asserted herein;

c. For damages in an amount to be determined by the trier of fact;

d. For an order of restitution and all other forms of equitable monetary relief;

e. Declaratory and injunctive relief as described herein;

f. Awarding Plaintiffs reasonable attorneys' fees, costs, and expenses as otherwise allowed by law;

g. Awarding pre- and post-judgment interest on any amounts awarded; and

h. Awarding such other and further relief as may be just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs, individually and on behalf of the putative Class, demand a trial by jury on all claims so triable.

Date: June 2, 2025

Respectfully Submitted,

EKSM, LLP

/s/ Leigh S. Montgomery
Leigh S. Montgomery
Texas Bar No. 24052214
lmontgomery@eksm.com
service@eksm.com
Jarrett L. Ellzey
Texas Bar No. 24040864
jellzey@eksm.com
4200 Montrose Street, Suite 200
Houston, Texas 77006
Phone: (888) 350-3931

Counsel for Plaintiff and Putative Class

JS 44 (Rev. 04/21) (TXND 4/21)

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

Susan Scott and Julian Cerna et al.,

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

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

EKSM, LLP, 4200 Montrose Blvd, Suite 200, Houston, Texas 77006 (888) 350-3931

DEFENDANTS

American National Bank & Trust

County of Residence of First Listed Defendant Wichita County, TX
(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 U.S.C. 1332 § (d)(2)

Brief description of cause:
Defendant suffered a data breach, which damaged a class of individuals whose personal information was stolen.

VII. REQUESTED IN COMPLAINT:

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

DEMAND $ 5,000,000.00

CHECK YES only if demanded in complaint:

JURY DEMAND: ☒ Yes ☐ No

VIII. RELATED CASE(S) IF ANY

(See instructions): JUDGE _____ DOCKET NUMBER 7:25-cv-00052

DATE 6/2/2025

SIGNATURE OF ATTORNEY OF RECORD s/Leigh S. Montgomery

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 a related case exists, whether pending or closed, insert the docket numbers and the corresponding judge names for such cases. A case is related to this filing if the case: 1) involves some or all of the same parties and is based on the same or similar claim; 2) involves the same property, transaction, or event; 3) involves substantially similar issues of law and fact; and/or 4) involves the same estate in a bankruptcy appeal.

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