UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

SANDRA HLADKY, *individually and on behalf of all others similarly situated*, Plaintiff, v. ABRI CREDIT UNION, Defendant.	Case No.: **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Sandra Hladkey ("Plaintiff"), individually and on behalf of all others similarly situated ("Class Members"), brings this Class Action Complaint against Defendant Abri Credit Union ("Defendant"), alleging as follows.

I. INTRODUCTION

1. This class action arises from Defendant's failure to properly secure and safeguard Plaintiff's and similarly situated Class Members' sensitive personally identifiable information ("PII"), which was stolen by cybercriminals in a foreseeable, preventable data breach.

2. In early May 2024, cybercriminals hacked into Defendant's network systems and stole Plaintiff's and Class Members' sensitive PII stored therein, including their full names, driver's license/government ID numbers, Social Security numbers, credit and debit card numbers, financial account information, and other confidential data (collectively, "Private Information"), causing widespread injuries and damages to Plaintiff and Class Members (the "Data Breach").

3. Defendant is a financial institution and one of the largest credit unions in Illinois, offering consumer banking, lending, and investment products

4. Plaintiff and Class Members are current and former customers of Defendant who received financial services from Defendant prior to the Data Breach. As a condition of obtaining Defendant's services, Plaintiff and Class Members were required to entrust their sensitive, confidential Private Information to Defendant, who stored and used Plaintiff's and Class Members' Private Information to provide and receive payment for its services.

5. Financial institutions that handle consumers' Private Information like Defendant owe the individuals to whom the information relates a duty to adopt reasonable measures to protect it from disclosure to unauthorized third parties, and to keep it safe and confidential. This duty arises under contract, statutory and common law, industry standards, representations made to Plaintiff and Class Members, and because it is foreseeable that the exposure of Private Information to unauthorized persons—and especially hackers with nefarious intentions—will harm the affected individuals, including but not limited to the invasion of their private health and financial matters.

6. In providing their Private Information to Defendant, Plaintiff and Class Members reasonably expected this sophisticated business entity to keep their Private Information confidential and security maintained, to use this information for business purposes, and to disclose it only as authorized. Defendant failed to do so, resulting in the unauthorized disclosure of Plaintiff's and Class Members' Private Information in the Data Breach.

7. Defendant breached its duties owed to Plaintiff and Class Members by failing to safeguard the Private Information it collected and maintained, including by failing to use adequate, reasonable, and legally-compliant data security measures to safeguard Plaintiff's and Class

Members' Private Information, which caused and allowed criminal hackers to access and steal thousands of individuals' Private Information in the Data Breach.

8. Upon information and belief, the mechanism of the cyberattack and potential for improper disclosure of Plaintiff's and Class Members' Private Information was a known risk to Defendant, and thus, Defendant knew that failing to take reasonable steps to secure the Private Information left it in a dangerous condition. Indeed, Defendant, a bank and financial services company bound to specific safeguards for PII under federal law, knew the importance of proper data protection and was on notice that its systems were vulnerable.

9. Defendant failed to adequately protect Plaintiff's and Class Members' Private Information—and failed to even encrypt or redact this highly sensitive data. This unencrypted, unredacted Private Information was compromised due to Defendant's negligent and/or careless acts and omissions and its utter failure to protect confidential customer PII.

10. Defendant breached its duties and obligations by failing, in one or more of the following ways: (a) to comply with industry-standard data security practices like encryption of PII in transit and storage; (b) to warn Plaintiff and Class Members of its inadequate data security practices; (c) to ensure legally compliant and industry standard data security measures to protect Private Information like multifactor authentication ("MFA"); (d) to use adequate monitoring and alerting methods, and consequentially failing to recognize or detect that Private Information network had been compromised and accessed until over 18 months after the Data Breach; (e) to utilize widely available software able to detect and prevent this type of attack; and (f) to otherwise secure the Private Information using reasonable and effective data security procedures free of foreseeable vulnerabilities and data security risks.

11. Hackers targeted and obtained Plaintiff's and Class Members' Private Information because of the data's value in exploiting and stealing their identities. As a direct and proximate result of Defendant's inadequate data security and breaches of its duties to handle Private Information with reasonable care, Plaintiff's and Class Members' Private Information was accessed by cybercriminals and exposed to an untold number of unauthorized individuals, and almost certainly published on the dark web. The present and continuing risk to Plaintiff and Class Members as victims of the Data Breach will remain for their respective lifetimes.

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

13. The risk of identity theft caused by this Data Breach is impending and has materialized, as there is evidence that the Plaintiff's and Class Members' Private Information was targeted, accessed, misused, and disseminated on the dark web.

14. As a result of the Data Breach, Plaintiff and Class Members suffered concrete injuries in fact including, but not limited to (a) financial costs incurred mitigating the materialized risk and imminent threat of identity theft; (b) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft; (c) actual identity theft and fraud; (d) financial costs incurred due to actual identity theft; (e) loss of time incurred due to actual identity theft; (f) deprivation of value of their Private Information; (g) loss of privacy; (h)

emotional distress including anxiety and stress in with dealing with the Data Breach; and (i) the continued risk to their sensitive Private Information, which remains in Defendant's possession and subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect it.

15. To recover for these harms, Plaintiff, on behalf of herself and the Class as defined herein, brings claims for negligence/negligence *per se*, breach of implied contract, and unjust enrichment, to address Defendant's inadequate safeguarding of Plaintiff's and Class Members' Private Information.

II. PARTIES

16. Plaintiff Sandra Hladkey is a natural person and a citizen and resident of Crest Hill, Illinois.

17. Defendant Abri Credit Union is a credit union chartered under Illinois law and with its headquarters and principal place of business at 1350 W. Renwick Road Romeoville, IL 60446.

III. JURISDICTION AND VENUE

18. This Court has subject matter jurisdiction over this action under 28 U.S.C.§ 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different than Defendant.

19. This Court has personal jurisdiction over Defendant because its principal place of business is in this state and Defendant regularly conducts business in this state.

20. Venue is proper under 18 U.S.C § 1391(b)(1) because Defendant resides in this District.

IV. GENERAL FACTUAL ALLEGATIONS

A. Defendant Collected, Maintained, and Shared Plaintiff's and Class Members' Private Information to Facilitate its Business, and Had Duties to Protect It.

21. Defendant is a financial institution that provides personal banking and financial services.

22. Plaintiff and Class Members are current and former customers of Defendant. As a condition of receiving Defendant's services, Plaintiff and Class Members were required to provide Defendant with their sensitive and non-public Private Information.

23. Defendant used Plaintiff's and Class Members' Private Information in its business to derive economic benefits, including for marketing purposes, and could not operate or profit without that data.

24. In exchange for receiving Plaintiff's and Class Members' Private Information, Defendant promised to safeguard the sensitive and confidential data, to use it only for authorized and legitimate purposes, and to delete such information from its systems once there was no longer a need to maintain it.

25. To that end, Defendant's Privacy Policy promised and assured Plaintiff and Class Members as follows:

> To protect your personal information from unauthorized access and use, we use security measures that comply with federal law. These measures include computer safeguards and secured files and buildings.
>
> We also maintain other physical, electronic and procedural safeguards to protect this information, and we limit access to information to those employees for whom access is appropriate.[1]

[1] https://www.abricu.com/bridge/disclosures/privacy/disclose.html.

26. Based on Defendant's express and implied representations and warranties and to obtain services from Defendant, Plaintiff and Class Members provided their Private Information to Defendant with the reasonable expectation and on the mutual understanding that Defendant would comply with its obligations to keep such information confidential and protected against unauthorized access. Consumers, in general, demand security for their Private Information, especially when Social Security numbers and sensitive financial data are involved.

27. Defendant had and continues to have duties to adopt reasonable measures to keep Plaintiff's and Class Members' Private Information confidential and protected from disclosure to unauthorized third parties, and to audit, monitor, and verify the integrity and cybersecurity of its systems.

28. Defendant had and has obligations stemming from the Federal Trade Commission ("FTC") Act, the Gramm-Leach-Bliley Act, 15 U.S.C. § 6801 ("GLBA"), common law, contract, and industry standards, to keep Plaintiff's and Class Members' Private Information confidential and protected from unauthorized disclosure.

29. Additionally, by obtaining, using, and benefitting from Plaintiff's and Class Members' Private Information, Defendant assumed legal and equitable duties and knew or should have known it was responsible for protecting that Private Information from unauthorized access and disclosure.

30. Defendant also owed a duty to protect Plaintiff and Class Members from the harm insufficient data security and the consequential exposure of Private Information would cause, because such harm was foreseeable and reasonably preventable.

31. Defendant knew it was storing valuable, sensitive Private Information and that as a result, its systems would be an attractive target for cybercriminals.

32. Defendant also knew that any breach of its network and exposure of the data stored therein would result in the increased risk of identity theft and fraud for the thousands of individuals whose Private Information was compromised, as well as intrusion into their private and sensitive financial matters.

33. Defendant's duty to protect Plaintiff and Class Members from the foreseeable risk of injury that inadequate data protection and unauthorized exposure of their Private Information would cause obligated Defendant to require and ensure it had implemented reasonable practices to keep Plaintiff's and Class Members' sensitive Private Information confidential and securely maintained, used and disclosed it for necessary and authorized purposes only, deleted the data from network systems or applications when no longer necessary for legitimate business purposes, and trained employees on reasonable cybersecurity red flags and protection techniques.

34. Defendant owed the foregoing duties to protect Private Information in its custody from unauthorized disclosure, and Defendant had the practical ability to fulfill those duties—yet, it failed to do so, causing the Data Breach.

35. The PII Defendant stored on its network systems when the Data Breach occurred, included the unencrypted Private Information of Plaintiff and Class Members.

B. Defendant's Failure to Adequately Safeguard Plaintiff's and Class Member's Private Information Caused the Data Breach.

36. In or around December 2025, Defendant began sending Plaintiff and other Data Breach victims correspondence titled 'Notice of Data Breach' ("Notice Letters").

37. The Notice Letters generally inform as follows:

> The privacy and security of the personal information we maintain is of the utmost importance to Abri Credit Union ("Abri"). We are writing with important information regarding a data security incident that involved some of your information. We want to provide you with information about the incident, explain the

> services we are making available to you, and let you know that we continue to take significant measures to protect your information.
>
> *What Happened?*
>
> Abri experienced unauthorized access to our network.
>
> *What We Are Doing.*
>
> Upon learning of this issue, we commenced a prompt and thorough investigation with external cybersecurity professionals experienced in handling these types of incidents. After an extensive forensic investigation and manual document review, we discovered on December 1, 2025 that the systems, which were accessed between May 3, 2024 and May 4, 2024, contained some of your personal information as described in more detail below.
>
> *What Information Was Involved?*
>
> The unauthorized actor accessed and/or acquired your full name and [PII].

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

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

40. The customer Private Information accessed and acquired by unauthorized actors in the Data Breach includes full names, driver's license/government ID numbers, Social Security numbers, credit and debit card numbers, financial account information, and other confidential data.

41. Plaintiff's and Class Members' Private Information was targeted, accessed, and stolen by cybercriminals in the Data Breach. Defendant's deficient security for customers' data caused and allowed criminals to target and take files containing Plaintiff's and Class Members' inadequately protected, unencrypted Private Information from Defendant's possession through the Data Breach.

42. As the Data Breach and its timeline evidences, Defendant did not use reasonable security measures appropriate to the nature of the sensitive Private Information Plaintiffs and Class Members provided it, such as encrypting the information; deleting the data when it was no longer needed; revoking employee user accounts' access to servers storing PII when such access was no longer needed; restricting access to the servers storing PII to only employees that are necessary and adequately trained to prevent unauthorized use of their login credentials; requiring sufficient verification such as MFA for user accounts to access servers storing PII; training employees about cybersecurity and attempts to gain unauthorized access; investigating and addressing vulnerabilities in its data security practices; and/or implementing the necessary safeguards to identify malicious activity. These failures allowed and caused cybercriminals to target Defendant's systems and carry out the Data Breach.

43. Defendant could and should have prevented this Data Breach by ensuring the files and servers containing Plaintiff's and Class Members' Private Information were properly secured, sanitized, and encrypted, but failed to do so.

44. Additionally, Defendant could have prevented this Data Breach by examining its cybersecurity protocols and ensuring vulnerabilities were identified and addressed and reasonable safeguards were continuously maintained, but failed to do so.

45. Defendant could and should have mplemented the following measures to prevent and detect the Data Breach, as recommended by the Microsoft Threat Protection Intelligence Team, but failed to do so:

> **Secure internet-facing assets**
> - Apply latest security updates
> - Use threat and vulnerability management
> - Perform regular audit; remove privileged credentials;
>
> **Include IT Pros in security discussions**
> - Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;
>
> **Build credential hygiene**
> - Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords;
>
> **Apply principle of least-privilege**
> - Monitor for adversarial activities
> - Hunt for brute force attempts
> - Monitor for cleanup of Event Logs
> - Analyze logon events.[2]

46. Defendant's negligence in safeguarding Plaintiff's and Class Members' Private Information is exacerbated by the repeated warnings and alerts regarding the need to protect and secure sensitive data.

C. Defendant Knew of the Risk of a Cyberattack because Financial Institutions in Possession of Private Information are Particularly Suspectable.

47. Defendant's negligence, including its gross negligence, in failing to safeguard Plaintiff's and Class Members' Private Information is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

[2] *See* Microsoft Threat Intelligence, *Human-operated ransomware attacks: A preventable disaster* (Mar. 5, 2020), https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster.

48. Private Information of the kind accessed in the Data Breach is of great value to cybercriminals as it can be used for a variety of unlawful and nefarious purposes, including ransomware, fraudulent misuse, and sale on the internet black market known as the dark web.

49. Private Information can also be used to distinguish, identify, or trace an individual's identity, such as his or her name, Social Security number, and financial records. This may be accomplished alone, or in combination with other personal or identifying information connected or linked to an individual such as his or her birthdate, birthplace, and mother's maiden name.

50. Data thieves regularly target entities that store Private Information like Defendant due to the highly sensitive information they maintain. Defendant knew and understood that Plaintiff's and Class Members' Private Information is valuable and highly sought after by criminal parties who seek to illegally monetize it through unauthorized access.

51. Cyberattacks against financial institutions such as Defendant are targeted and frequent. According to Contrast Security's 2023 report, "Cyber Bank Heists: Threats to the financial sector," "[o]ver the past year, attacks have included banking trojans, ransomware, account takeover, theft of client data and cybercrime cartels deploying 'trojanized' finance apps to deliver malware in spear-phishing campaigns."[3]

52. According to the Identity Theft Resource Center's report covering the year 2021, "the overall number of data compromises (1,862) is up more than 68 percent compared to 2020. The new record number of data compromises is 23 percent over the previous all-time high (1,506)

[3] Tom Kellermann, *Cyber Bank Heists: Threats to the financial sector*, at 5, CONTRAST SECURITY https://www.contrastsecurity.com/hubfs/Cyber%20Bank%20Heists%20Report%2020 23.pdf (last accessed Oct. 10, 2024).

set in 2017. The number of data events that involved sensitive information (Ex: Social Security numbers) increased slightly compared to 2020 (83 percent vs. 80 percent)."[4]

53. The increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendant's industry, including Defendant itself. According to IBM's 2022 report, "[f]or 83% of companies, it's not if a data breach will happen, but when."[5]

54. Defendant knew or should have known of the inherent risks in collecting and storing Private Information and the critical importance of providing adequate security for it.

55. As a financial institution in possession of consumers' Private Information, Defendant knew, or should have known, the importance of safeguarding the Private Information entrusted to it by Plaintiff and Class Members and of the foreseeable consequences if its network systems were breached. Such consequences include the significant costs imposed on Plaintiff and Class Members due to a breach. Nevertheless, Defendant failed to implement or follow reasonable cybersecurity measures to protect against the Data Breach.

56. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the Private Information of Plaintiff and Class Members from being compromised.

57. Defendant was, or should have been, fully aware of the unique type and the significant volume of its customers' Private Information on its server, and, thus, the thousands of individuals who would be harmed by the unauthorized exposure of that unencrypted data.

---

[4] *See* Identity Theft Res. Ctr., *2021 Annual Data Breach Report Sets New Record for Number of Compromises*, ITRC (Jan. 24, 2022), https://www.idtheftcenter.org/post/identity-theft-resource-center-2021-annual-data-breach-report-sets-new-record-for-number-of-compromises.

[5] IBM, *Cost of a data breach 2022: A million-dollar race to detect and respond*, https://www.ibm.com/reports/data-breach (last accessed Oct. 10, 2024).

58. Given the nature of the Data Breach, it was foreseeable that Plaintiff's and Class Members' Private Information compromised therein would be targeted by hackers and cybercriminals for use in variety of different injurious ways. Indeed, the cybercriminals who possess Plaintiff's and Class Members' Private Information can easily obtain their tax returns or open fraudulent credit card accounts in Plaintiff's and Class Members' names.

59. Plaintiff and Class Members were the foreseeable and probable victims of Defendant's inadequate security practices and procedures. The breadth of data compromised in the Data Breach makes the information particularly valuable to thieves and leaves Plaintiff and Class Members especially vulnerable to identity theft, financial fraud, and the like.

D. Defendant Was Required, But Failed, to Comply with FTC Rules and Guidance.

60. 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.

61. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which establishes cyber-security guidelines for businesses like Defendant. These guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.

62. The FTC's guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

63. The FTC further recommends that companies not maintain Private 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.

64. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect third parties' confidential 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 business like Defendant must undertake to meet their data security obligations.

65. Such FTC enforcement actions include actions against businesses that fail to use adequate data security practices like Defendant. *See, e.g.*, *In the Matter of LabMD, Inc.*, 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.").

66. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect Private Information. The FTC publications and orders described above also form part of the basis of Defendant's duties in this regard.

67. The FTC has also recognized that consumer data is a new and valuable form of currency. In an FTC roundtable presentation, former Commissioner Pamela Jones Harbour stated

that "most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis and profit."

68. Defendant failed to properly implement basic data security practices, in violation of its duties under the FTC Act.

69. Defendant's failures to employ reasonable and appropriate means to protect against unauthorized access to Plaintiff's and Class Members' Private Information or to comply with applicable industry standards constitutes an unfair act or practice prohibited by the FTC Act.

70. Additionally, Defendant is a financial institution for purposes of the GLBA, 15 U.S.C. § 6801, because it is "significantly engaged in financial activities, or significantly engaged in activities incidental to such financial activities." 16 C.F.R. § 314.2(h).

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

72. The PII involved in the Data Breach constitutes "nonpublic personal information" for purposes of the GLBA.

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

74. The FTC's Safeguards Rule, which implements Section 501(b) of the GLBA, 15 U.S.C. § 6801(b), requires financial institutions to protect the security, confidentiality, and

integrity of customer information by developing a comprehensive written information security program that contains reasonable administrative, technical, and physical safeguards, including: (i) designating one or more employees to coordinate the information security program; (ii) identifying reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information, and assessing the sufficiency of any safeguards in place to control those risks; (iii) designing and implementing information safeguards to control the risks identified through risk assessment, and regularly testing or otherwise monitoring the effectiveness of the safeguards' key controls, systems, and procedures; (iv) overseeing service providers and requiring them by contract to protect the security and confidentiality of customer information; and (v) evaluating and adjusting the information security program in light of the results of testing and monitoring, changes to the business operation, and other relevant circumstances. 16 C.F.R. §§ 314.3 & 314.4. As alleged herein, Defendant violated the Safeguards Rule.

75. Defendant's conduct resulted in a variety of failures to follow the Safeguards Rule's requirements, many of which are also industry standard. Foremost among such deficient practices, Defendant's failure to discover that the Data Breach compromised Plaintiff's and Class Members' Private Information until ***over 18 months*** later demonstrates that Defendant failed to design and implement information safeguards to control the risks identified through risk assessment, and regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures.

76. Had Defendant complied with the Safeguards Rule and ensured it implemented data security protocols, the Data Breach would have been avoided, or its resulting damage to Plaintiff and the Class at least significantly reduced, as the Data Breach could have been detected earlier, the amount of Private Information compromised could have been greatly lessened.

E. Defendant Failed to Comply with Industry Standards.

77. A number of published industry and national best practices are widely used as a go-to resource when developing an institution's cybersecurity standards.

78. The Center for Internet Security's (CIS) Critical Security Controls (CSC) recommends certain best practices to adequately secure data and prevent cybersecurity attacks, including Critical Security Controls of Inventory and Control of Enterprise Assets, Inventory and Control of Software Assets, Data Protection, Secure Configuration of Enterprise Assets and Software, Account Management, Access Control Management, Continuous Vulnerability Management, Audit Log Management, Email and Web Browser Protections, Malware Defenses, Data Recovery, Network Infrastructure Management, Network Monitoring and Defense, Security Awareness and Skills Training, Service Provider Management, Application Software Security, Incident Response Management, and Penetration Testing.

79. The National Institute of Standards and Technology ("NIST") also recommends certain practices to safeguard systems, such as the following:

a. Control who logs on to your network and uses your computers and other devices.

b. Use security software to protect data.

c. Encrypt sensitive data, at rest and in transit.

d. Conduct regular backups of data.

e. Update security software regularly, automating those updates if possible.

f. Have formal policies for safely disposing of electronic files and old devices.

g. Train everyone who uses your computers, devices, and network about cybersecurity. You can help employees understand their personal risk in addition to their crucial role in the workplace.

80. Further still, CISA makes specific recommendations to organizations to guard against cybersecurity attacks, including (a) reducing the likelihood of a damaging cyber intrusion by validating that "remote access to the organization's network and privileged or administrative access requires multi-factor authentication, [e]nsur[ing] that software is up to date, prioritizing updates that address known exploited vulnerabilities identified by CISA[,] [c]onfirm[ing] that the organization's IT personnel have disabled all ports and protocols that are not essential for business purposes," and other steps; (b) taking steps to quickly detect a potential intrusion, including "[e]nsur[ing] that cybersecurity/IT personnel are focused on identifying and quickly assessing any unexpected or unusual network behavior [and] [e]nabl[ing] logging in order to better investigate issues or events[;] [c]onfirm[ing] that the organization's entire network is protected by antivirus/antimalware software and that signatures in these tools are updated," and (c) "[e]nsur[ing] that the organization is prepared to respond if an intrusion occurs," and other steps.

81. Upon information and belief, Defendant failed to implement industry-standard cybersecurity measures, including by failing to meet the minimum standards of both the NIST Cybersecurity Framework Version 2.0 (including 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 established frameworks for reasonable cybersecurity readiness, and by failing to comply with other industry standards for protecting Plaintiff's and Class Members' Private Information, resulting in the Data Breach.

F. Defendant Owed Plaintiff and Class Members a Common Law Duty to Safeguard their Private Information.

82. In addition to its obligations under federal and state laws, Defendant owed a common law duty to Plaintiff and Class Members to exercise reasonable care in obtaining,

retaining, securing, safeguarding, deleting, and protecting the Private Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendant's duty owed to Plaintiff and Class Members obligated it to provide reasonable data security, including consistency with industry standards and requirements, and to ensure that the servers, networks, and protocols storing Plaintiff's and Class Members' Private Information adequately protected it.

83. Defendant owed a duty to Plaintiff and Class Members to create and implement reasonable data security practices and procedures to protect the Private Information in its custody.

84. Defendant owed a duty to Plaintiff and Class Members to implement processes that would detect a compromise of Private Information in a timely manner.

85. Defendant owed a duty to Plaintiff and Class Members to act upon data security warnings and alerts in a timely fashion.

86. Defendant owed a duty to Plaintiff and Class Members to disclose in a timely and accurate manner when and how the Data Breach occurred.

87. Defendant owed these duties of care to Plaintiff and Class Members because they were foreseeable and probable victims of any inadequate data security practices.

88. Defendant tortiously failed to take precautions required to safeguard and protect Plaintiff's and Class Members' Private Information from unauthorized disclosure. Defendant's actions and omissions represent a flagrant disregard of Plaintiff's and Class Members' rights.

J. Plaintiff and Class Members Suffered Common Injuries and Damages.

89. Defendant's failure to ensure adequate data security measures for Plaintiff's and Class Members' Private Information directly and proximately caused injuries to Plaintiff and Class Members by the resulting disclosure of their Private Information in the Data Breach.

90. The ramifications of Defendant's failures to keep secure the Private Information of Plaintiff and Class Members are long lasting and severe. Once Private Information is stolen fraudulent use of that information and damage to victims may continue for years.

91. Plaintiff and Class Members are also at a continued risk because their Private Information remains on Defendant's server, which has already been shown to be susceptible to compromise and is subject to further attack so long as Defendant fails to undertake the necessary and appropriate security measures to protect consumers' Private Information in its care.

92. As a result of Defendant's ineffective and inadequate data security practices, the consequential Data Breach, and the foreseeable outcome of Plaintiff's and Class Members' Private Information ending up in criminals' possession, all Plaintiff and Class Members have suffered and will continue to suffer the following actual injuries and damages, without limitation (a) invasion of privacy; (b) financial costs incurred mitigating the materialized risk and imminent threat of identity theft; (c) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft; (d) financial costs incurred due to actual identity theft; (e) loss of time incurred due to actual identity theft; (f) deprivation of value of their Private Information; (g) emotional distress including anxiety and stress in dealing with the Data Breach's aftermath; and (i) the continued risk to their sensitive Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect it.

Present and Ongoing Risk of Identity Theft to Plaintiff and Class Members

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

94. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal Private Information to monetize it. Criminals monetize the data by selling the stolen information on the internet black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

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

96. A sophisticated black market exists on the dark web where criminals can buy or sell malware, firearms, drugs, and frequently, PII like the Private Information at issue here. The digital character of Private Information stolen in data breaches lends itself to dark web transactions because it is immediately transmissible over the internet and the buyer and seller can retain their anonymity. The sale of a firearm or drugs on the other hand requires a physical delivery address. Nefarious actors can readily purchase usernames and passwords for online streaming services, stolen financial information and account login credentials, and Social Security numbers, dates of birth, and medical information.

97. The unencrypted Private Information of Plaintiff and Class Members will end up for sale on the dark web because that is the *modus operandi* of hackers. In addition, unencrypted and detailed Private Information may fall into the hands of companies that will use it for targeted

marketing without the approval of Plaintiff and Class Members. Unauthorized actors can easily access and misuse Plaintiff's and Class Members' Private Information due to the Data Breach.

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

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[6]

99. According to the Social Security Administration, each time an individual's Social Security number is compromised, "the potential for a thief to illegitimately gain access to bank accounts, credit cards, driving records, tax and employment histories and other private information increases."[7] Moreover, "[b]ecause many organizations still use SSNs as the primary identifier, exposure to identity theft and fraud remains."[8]

100. In fact, "[a] stolen Social Security number is one of the leading causes of identity theft and can threaten your financial health."[9] Someone who has your SSN can use it to

---

[6] Social Security Admin., Pub. No. 06-10064, *Identity Theft and Your Social Security Number* (June 2021), https://www.ssa.gov/pubs/EN-05-10064.pdf.

[7] *See* Social Security Admin., *Avoid Identity Theft: Protect Social Security Numbers*, https://www.ssa.gov/phila/ProtectingSSNs.htm (last visited Oct. 10, 2024).

[8] *Id.*

[9] *See How to Protect Yourself from Social Security Number Identity Theft*, EQUIFAX https://www.equifax.com/personal/education/identity-theft/articles/-/learn/social-security-number-identity-theft (last visited Oct. 10, 2024).

impersonate you, obtain credit and open bank accounts, apply for jobs, steal your tax refunds, get medical treatment, and steal your government benefits.

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

102. Even then, new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[10]

103. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant issued in the victim's name. And the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for credit lines.

104. For these reasons, some courts have referred to Social Security numbers as the "gold standard" for identity theft. *Portier v. NEO Tech. Sols*., No. 3:17-CV-30111, 2019 WL 7946103, at *12 (D. Mass. Dec. 31, 2019) ("Because Social Security numbers are the gold standard

[10] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last visited Aug. 23, 2024).

for identity theft, their theft is significant . . . . Access to Social Security numbers causes long-lasting jeopardy because the Social Security Administration does not normally replace Social Security numbers."); *see also McFarlane v. Altice USA, Inc*., 524 F. Supp. 3d 264, 272 (S.D.N.Y. Mar. 8, 2021) (noting that Social Security numbers are: arguably "the most dangerous type of personal information in the hands of identity thieves"; Unlike a credit card number, which can be changed to eliminate the risk of harm following a data breach, "[a] social security number derives its value in that it is immutable," and when stolen can "forever be wielded to identify [the victim] and target his in fraudulent schemes and identity theft attacks.").

105. Similarly, California's Attorney General warns consumers: "Originally, your Social Security number (SSN) was a way for the government to track your earnings and pay you retirement benefits. But over the years, it has become much more than that. It is the key to a lot of your personal information. With your name and SSN, an identity thief could open new credit and bank accounts, rent an apartment, or even get a job."[11]

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

107. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate and trick individuals into disclosing additional confidential or personal information through means

[11] *See* Office of the Attorney General of Cal., *Your Social Security Number: Controlling the Key to Identity Theft*, https://oag.ca.gov/idtheft/facts/your-ssn (last visited Oct. 10, 2024).

such as spam phone calls and text messages or phishing emails. Data breaches are often the starting point for these additional targeted attacks on the victims.

108. One such example of criminals piecing together bits and pieces of compromised Private Information for profit is the development of "Fullz" packages.[12]

109. With Fullz packages, cyber-criminals can cross-reference two sources of Private Information to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy to assemble complete dossiers on individuals. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the Private Information that was exfiltrated in the Data Breach, criminals may still easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

110. The development of Fullz packages means that stolen Private Information from the Data Breach can easily be used to link and identify it to Plaintiff's and Class Members' phone numbers, email addresses, and other unregulated sources and identifiers. That is exactly what is happening to Plaintiff and Class Members, and it is reasonable for any trier of fact, including this

[12] "Fullz" is fraudster speak for data that includes the victim's information, including but not limited to name, address, credit card information, Social Security number, date of birth, and more. As a rule of thumb, the more information on a victim, the more money that can be made off those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See*, *e.g.*, Brian Krebs, *Medical Recs. for Sale in Underground Stolen from Texas Life Ins. Firm*, Krebs on Security (Sep. 18, 2014), https://krebsonsecuritv.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-firm.

Court or a jury, to find that their stolen Private Information is being misused, and that such misuse is traceable to the Data Breach.

111. Victims of identity theft suffer from both direct and indirect financial losses. According to a research study published by the Department of Justice,

> A direct financial loss is the monetary amount the offender obtained from misusing the victim's account or personal information, including the estimated value of goods, services, or cash obtained. It includes both out-of-pocket loss and any losses that were reimbursed to the victim. An indirect loss includes any other monetary cost caused by the identity theft, such as legal fees, bounced checks, and other miscellaneous expenses that are not reimbursed (e.g., postage, phone calls, or notary fees). All indirect losses are included in the calculation of out-of-pocket loss.[13]

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

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

114. In addition to out-of-pocket expenses that can exceed thousands of dollars and the emotional toll identity theft can take, some victims must spend a considerable time repairing the damage caused by the theft of their Private Information. Victims of new account identity theft will likely have to spend time correcting fraudulent information in their credit reports and continuously monitor their reports for future inaccuracies, close existing bank/credit accounts, open new ones, and dispute charges with creditors.

---

[13] Erika Harrell, *Bureau of Just. Stat.*, U.S. DEP'T OF JUST., NCJ 256085, *Victims of Identity Theft*, 2018 I (2020) https://bjs.ojp.gov/content/pub/pdf/vit18.pdf.

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

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

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

117. In the event that Plaintiff and Class Members experience actual identity theft and fraud, the United States Government Accountability Office released a report in 2007 regarding data breaches in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[14]

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

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

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

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

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

Diminished Value of Private Information

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

123. For example, drug and medical device manufacturers, pharmacies, hospitals, and other healthcare service providers often purchase Private Information on the black market for the purpose of target-marketing their products and services to the physical maladies of the data breach victims themselves.

124. Private Information can sell for as much as $363 per record according to the Infosec Institute.

125. An active and robust legitimate marketplace for Private Information also exists. In 2019, the data brokering industry was worth roughly $200 billion. In fact, the data marketplace is

so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers. Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50 a year.

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

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

Reasonable and Necessary Future Cost of Credit and Identify Theft Monitoring

128. To date, Defendant has done nothing to provide Plaintiff and Class Members with relief for the damages they have suffered due to the Data Breach.

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

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

131. Furthermore, the information accessed and disseminated in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, where victims can easily cancel or close credit and debit card accounts. The information disclosed in this Data Breach is impossible to "close" and difficult, if not impossible, to change (such as Social Security numbers). Consequently, Plaintiff and Class Members are at a present and ongoing risk of fraud and identity theft for many years into the future, if not forever.

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

Loss of Benefit of the Bargain

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

134. When agreeing to provide their Private Information, which was a condition precedent to obtain banking services from Defendant, and paying Defendant, directly or indirectly, for these products and services, Plaintiff and Class Members as consumers understood and

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

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

V. PLAINTIFF'S EXPERIENCES AND INJURIES

136. As a condition of receiving or applying for banking or related financial services from Defendant, Plaintiff was required to supply Defendant with her Private Information.

137. Plaintiff greatly values her privacy and is very careful about sharing her sensitive Private Information. Plaintiff diligently protects her Private Information and stores any documents containing Private Information in a safe and secure location. She has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

138. At the time of the Data Breach, Defendant retained Plaintiff's Private Information on its network systems with inadequate data security, causing Plaintiff's Private Information to be accessed and exfiltrated by cybercriminals in the Data Breach.

139. As a result of the Data Breach, Plaintiff has made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching and verifying the legitimacy and underlying facts of the Data Breach, reviewing account statements and credit histories, and other mitigation efforts—valuable time she otherwise would have spent on other like work and/or recreation. This time has been lost forever and cannot be recaptured.

140. Plaintiff further anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. Due to the Data Breach,

Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

141. The risk of identity theft is impending and has materialized, as there is evidence that Plaintiff's and Class Members' Private Information was targeted by cybercriminals, accessed, stolen, and misused, including through dissemination on the dark web.

142. Plaintiff further believes her Private Information, and that of Class Members, was and will be sold and disseminated on the dark web following the Data Breach as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type

143. Plaintiff has additionally suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breach, given that cybercriminals are able to easily use the information compromised in the Data Breach to find more information about an individual, such as his phone number or email address, from publicly available sources, including websites that aggregate and associate personal information with the owner of such information.

144. The Data Breach has caused Plaintiff to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant took over 18 months to notify her about the Data Breach, and has still not fully informed her of key details about the Data Breach's occurrence.

VI. CLASS ACTION ALLEGATIONS

145. Plaintiff brings this nationwide class action individually and on behalf of all others similarly situated pursuant to Federal Rule of Civil Procedure 23(b)(2), 23(b)(3), and 23(c)(4).

146. The class Plaintiff seek to represent is defined as follows ("Class"):

> All individuals in the United States whose Private Information may have been compromised in the Data Breach, including all individuals who received a Notice Letter from Defendant.

147. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

148. Plaintiff reserves the right to amend the definitions of the Class or add a Class or Subclass if further information and discovery indicate that the definitions of the Class should be narrowed, expanded, or otherwise modified.

149. Numerosity. The members of the Class are so numerous that joinder of all members is impracticable, if not completely impossible. Although the precise number of individuals is currently unknown to Plaintiff and exclusively in the possession of Defendant, upon information and belief, the number of Class Members is over 14,000. The Class is identifiable within Defendant's records, and Defendant has already identified these individuals (as evidenced by sending them Notice Letters).

150. Common questions of law and fact exist as to all members of the Class and predominate over any questions affecting solely individual members of the Class. Among the questions of law and fact common to the Class that predominate over questions which may affect individual Class members, including the following:

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

b. Whether Defendant had a duty not to disclose the Private Information of Plaintiff and Class Members to unauthorized third parties;

c. Whether Defendant failed to adequately safeguard the Private Information of Plaintiff and Class Members;

d. Whether and when Defendant actually learned of the Data Breach;

e. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their Private Information had been compromised;

f. Whether Defendant violated the law by failing to promptly notify Plaintiff and Class Members that their Private Information had been compromised;

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

h. Whether Defendant adequately addressed the vulnerabilities which permitted the Data Breach to occur;

i. Whether Plaintiff and Class Members are entitled to actual damages, compensatory damages, punitive damages, and/or nominal damages as a result of Defendant's wrongful conduct; and

j. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

151. Typicality. Plaintiff's claims are typical of those of the other members of the Class because Plaintiff, like every other Class Member, was exposed to virtually identical conduct and now suffers from the same violations of the law as each other member of the Class.

152. Adequacy. Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that she has no disabling conflicts of interest that would be antagonistic to those of the other Class Members. Plaintiff seeks no relief that is antagonistic or adverse to the

Class Members and the infringement of the rights and the damages she has suffered are typical of other Class Members. Plaintiff has retained counsel experienced in complex class action and data breach litigation, and Plaintiff intends to prosecute this action vigorously.

153. Superiority and Manageability. The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

154. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since it would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff was exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

155. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

156. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

157. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the Private Information of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendant may continue to act unlawfully as set forth in this Complaint.

158. Policies Generally Applicable to the Class. This class action is also appropriate for certification because Defendant acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief and corresponding declaratory relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiff's challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

VII. CAUSES OF ACTION

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

159. Plaintiff re-alleges and incorporates by reference paragraphs 1 through 158 above as if fully set forth herein.

160. Defendant required Plaintiff and Class Members to submit confidential Private Information to Defendant as a condition of receiving Defendant's services.

161. Plaintiff and Class Members provided their Private Information to Defendant prior to the Data Breach in exchange for receiving Defendant's services.

162. Defendant had full knowledge of the sensitivity of the Private Information entrusted to it, and the types of harm that Plaintiff and Class Members could and would suffer if the Private Information was wrongfully disclosed to unauthorized persons. Defendant had duties to Plaintiff and each Class Member to exercise reasonable care in holding, safeguarding, and protecting their Private Information.

163. Plaintiff and Class Members were the foreseeable victims of any inadequate safety and security practices by Defendant.

164. Plaintiff and Class Members had no ability to protect their Private Information in Defendant's possession.

165. By collecting, storing, and benefitting from Plaintiff's and Class Members' Private Information, Defendant had a duty of care to require and ensure reasonable means to secure and safeguard the data, prevented its disclosure, and safeguarded the Private Information from theft.

166. Defendant's duty of care obligated it to use processes by which it could detect if its network was breached or if Private Information was exposed to unauthorized actors.

167. Defendant's duty of care further obligated it to maintain processes sufficient to detect unauthorized access to its network or compromises of Private Information stored therein.

168. Defendant owed a duty to Plaintiff and Class Members to implement and maintain data security measures consistent with industry standards and legal and regulatory requirements,

to ensure that its systems and servers and the people and entities with access to them adequately protected Plaintiff's and Class Members' Private Information.

169. Defendant was able to ensure its data security procedures were sufficient to protect against the foreseeable risk of harm to Plaintiff and Class Members from a cybersecurity event like this Data Breach, whereas Plaintiff and Class Members were not.

170. Defendant had a duty to employ reasonable security measures under Section 5 of the FTC 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.

171. Pursuant to the FTC Act, 15 U.S.C. § 45, Defendant had a duty to provide adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Private Information.

172. Additionally, pursuant to the GLBA and the FTC Safeguards Rule, which implements Section 501(b) of the GLBA, Defendant had a duty to protect the security, confidentiality, and integrity of customer information by developing a comprehensive written information security program that contains reasonable administrative, technical, and physical safeguards, including identifying reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information, and assessing the sufficiency of any safeguards in place to control those risks. 16 C.F.R. §§ 314.3 & 314.4.

173. Defendant's conduct resulted in a variety of failures to follow the Safeguards Rule's requirements, many of which are also industry standard. Foremost among such deficient practices, Defendant's failure to discover that the Data Breach compromised Plaintiff's and Class Members' Private Information until ***over 18 months*** later demonstrates that Defendant failed to design and

implement information safeguards to control the risks identified through risk assessment, and regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures.

174. Had Defendant complied with the Safeguards Rule and ensured it implemented data security protocols, the Data Breach would have been avoided, or its resulting damage to Plaintiff and the Class at least significantly reduced, as the Data Breach could have been detected earlier, the amount of Private Information compromised could have been greatly lessened

175. Defendant's violations of the FTC Act and the Safeguards Rule as described herein directly caused and/or were a substantial factor in the Data Breach and resulting injuries to Plaintiff and Class Members.

176. Plaintiff and Class Members are within the class of persons the FTC Act and the Safeguards Rule were intended to protect.

177. The type of harm that resulted from the Data Breach was the type of harm the FTC Act and the Safeguards Rule were intended to guard against.

178. Defendant's failures to comply with the FTC Act and the Safeguards Rule is negligence *per se* and/or prima facie evidence of negligence.

179. Defendant's duties to use reasonable care in protecting Plaintiff's and Class Members' Private Information arose not only as a result of the statutes and regulations described above, but because Defendant is bound by industry standards to secure such Private Information.

180. Defendant breached its duties and was negligent by failing to use reasonable measures to protect Plaintiff's and Class Members' Private Information from unauthorized disclosure in the Data Breach. The specific negligent acts and omissions committed by Defendant are detailed *supra* and include, but are not limited to, the following:

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

b. Failing to implement and maintain cybersecurity practices that could detect and protect against unauthorized access to or use of Private Information;

c. Failing to adequately monitor or supervise its data security practices; and

d. Failure to periodically ensure it had plans in place to maintain reasonable data security safeguards, or to adequately test those plans.

181. But for Defendant's wrongful and negligent breaches of duties owed to Plaintiff and Class Members, the Data Breach would not have occurred or at least would have been mitigated, Plaintiff's and Class Members' Private Information would not have been compromised, and Plaintiff's and Class Members' injuries would have been avoided.

182. It was foreseeable that Defendant's failures to use reasonable measures to protect Plaintiff's and Class Members' Private Information would injure Plaintiff and Class Members. Further, the breach of security was reasonably foreseeable to Defendant given the known high frequency of cyber-attacks and data breaches in Defendant's industry.

183. It was therefore foreseeable that the failure to adequately safeguard Plaintiff's and Class Members' Private Information would cause them one or more types of injuries.

184. As a direct and proximate result of Defendant's negligence, Plaintiff and Class Members have suffered and will suffer injuries and damages, including but not limited to (a) invasion of privacy; (b) lost or diminished value of their Private Information; (c) actual identity theft and fraud; (d) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; (e) loss of benefit of their bargain; and (f) the continued and certainly increased risk to their Private Information, which

remains in Defendant's possession and subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect it.

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

186. Plaintiff and Class Members are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

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

187. Plaintiff re-alleges and incorporates by reference paragraphs 1 through 158 above as if fully set forth herein.

188. Defendant required Plaintiff and Class Members to provide and entrust their Private Information to Defendant as a condition of obtaining Defendant's banking and financial services.

189. When Plaintiff and Class Members provided their Private Information to Defendant, they entered into implied contracts with Defendant pursuant to which Defendant agreed to safeguard and protect such Private Information.

190. Specifically, Plaintiff and Class Members entered into valid and enforceable implied contracts with Defendant when they agreed to provide their Private Information and/or payment to Defendant.

191. The valid and enforceable implied contracts that Plaintiff and Class Members entered into with Defendant included Defendant's promises to protect Private Information it collected from Plaintiff and Class Members, or created on its own, from unauthorized disclosures

through reasonable and legally compliant safeguards. Plaintiff and Class Members provided this Private Information in reliance on Defendant's promises.

192. Under the implied contracts, Defendant promised and was obligated to (a) provide banking services to Plaintiff and Class Members; and (b) protect Plaintiff's and Class Members' Private Information provided to obtain such services and/or created in connection therewith. In exchange, Plaintiff and Class Members agreed to provide Defendant with payment and their Private Information.

193. Defendant promised and warranted to Plaintiff and Class Members, including through its public-facing Privacy Notice identified above, to maintain the privacy and confidentiality of the Private Information it collected from Plaintiff and Class Members and to keep such information safeguarded against unauthorized access and disclosure.

194. Defendant's adequate protection of Plaintiff's and Class Members' Private Information was a material aspect of these implied contracts.

195. Defendant solicited and invited Plaintiff and Class Members to provide their Private Information as part of Defendant's regular business practices. Plaintiff and Class Members accepted Defendant's offers and provided their Private Information to Defendant.

196. In entering into such implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendant's data security practices complied with industry standards and relevant laws and regulations, including the FTC Act, the GLBA and the Safeguards Rule, and industry standards.

197. A meeting of the minds occurred when Defendant required Plaintiff and the Class Members to provide their Private Information as a mandatory condition to their receipt of services

and when Plaintiff and Class Members agreed to, and did, provide their Private Information to Defendant.

198. Plaintiff and Class Members performed their obligations under the contracts when they provided their Private Information and/or payment to Defendant.

199. Defendant materially breached its contractual obligations to protect the Private Information it required Plaintiff and Class Members to provide when that Private Information was unauthorizedly disclosed in the Data Breach due to Defendant's inadequate data security measures and procedures.

200. Defendant materially breached the terms of its implied contracts, including but not limited to by failing to comply with industry standards or the standards of conduct embodied in laws like Section 5 of the FTC Act, the GLBA, and the Safeguards Rule and by failing to otherwise protect Plaintiff's and Class Members' Private Information, as set forth *supra*.

201. The Data Breach was a reasonably foreseeable consequence of Defendant's conduct, by acts of omission or commission, in breach of these implied contracts with Plaintiff and Class Members.

202. As a result of Defendant's failures to fulfill the data security protections promised, Plaintiff and Class Members did not receive the full benefit of their bargains with Defendant, and instead received services of a diminished value compared to that described in the implied contracts. Plaintiff and Class Members were therefore damaged in an amount at least equal to the difference in the value of the services with data security protection they paid for and that which they received.

203. Had Defendant disclosed that its data security procedures were inadequate or that they did not adhere to applicable law or industry-standards for cybersecurity, neither Plaintiff,

Class Members, nor any reasonable person would have contracted with or provided Private Information Defendant.

204. As a direct and proximate result of Defendant's breach of their implied contracts with Plaintiff and Class Members and the consequential Data Breach, Plaintiff and Class Members have suffered injuries and damages as set forth herein and have been irreparably harmed, as well as suffering and the loss of the benefit of the bargain they struck with Defendant.

205. Plaintiff and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, and/or restitution, in an amount to be proven at trial

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

206. Plaintiff re-alleges and incorporates by reference paragraphs 1 through 158 above as if fully set forth herein.

207. Plaintiff and Class Members conferred a monetary benefit on Defendant. Specifically, they provided their payment and their Private Information to Defendant. In exchange, Plaintiff and Class Members should have had their Private Information protected with adequate data security.

208. Defendant knew Plaintiff and Class Members conferred a benefit upon it and accepted and retained that benefit by accepting, retaining, using, and profiting off managing the Private Information entrusted to it. Defendant profited from Plaintiff's retained data and used Plaintiff's and Class Members' Private Information for business purposes and to generate revenue, including by using the Private Information for marketing and analytics purposes.

209. Defendant failed to use reasonable or adequate measures to secure Plaintiff's and Class Members' Private Information and, therefore, did not fully compensate Plaintiff or Class Members for the value that their Private Information provided.

210. Defendant acquired the Private Information through inequitable record retention as they failed to investigate and/or disclose the inadequate data security practices previously alleged.

211. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures, while profiting from that same PII. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant calculated to increase its own profits at the expense of Plaintiff and Class Members by using cheaper, ineffective security measures, and diverting those funds to Defendant's own pocket.

212. Plaintiff 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 customers' Private Information.

213. Under the circumstances, it would be unjust for Defendant to be permitted to retain any of the benefits that Plaintiff and Class Members conferred upon it.

214. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injuries and damages as set forth herein.

215. Plaintiff 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 for its wrongful conduct. This can be accomplished by establishing a constructive trust from which the Plaintiff and Class Members may seek restitution or compensation.

VIII. PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all similarly situated Class Members, prays for judgment against Defendant and requests from the Court the following:

A. For an order certifying the Class, as defined herein, and appointing Plaintiff and her Counsel to represent the Class;

B. For an award of damages, including actual, nominal, and consequential damages, as allowed by law in an amount to be determined at trial;

C. For an award of attorneys' fees and costs as allowed by law;

D. For prejudgment interest on all amounts awarded; and

E. Such other and further relief as this Court may deem just and proper.

IX. JURY TRIAL DEMANDED

Plaintiff, individually and on behalf of the Class, hereby demands a trial by jury on all claims so triable.

Dated: January 12, 2026

Respectfully submitted,

By: *[/s/ Jeff Ostrow](#)*
Jeff Ostrow
KOPELOWITZ OSTROW P.A.
One West Las Olas Blvd., Suite 500
Fort Lauderdale, FL 33301
Tel: 954-525-4100
ostrow@kolawyers.com

Counsel for Plaintiff and the Putative Class

CIVIL COVER SHEET

The ILND 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

Sandra Hladky,

(b) County of Residence of First Listed Plaintiff Will County, IL
(Except in U.S. plaintiff cases)

(c) Attorneys *(firm name, address, and telephone number)*

Kopelowitz Ostrow PA, 1 W. Las Olas Blvd, Ste. 500, Ft. Lauderdale FL 33301 / Tel: 954-525-4100

DEFENDANTS

Abri 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 *(Check **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 *(For Diversity Cases Only.)*

*(Check **one** box, only for plaintiff and **one** box for defendant.)*

	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 *(Check **one** box, only.)*

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 Loan (Excludes Veterans)
- ☐ 153 Recovery 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

PRISONER PETITIONS

- ☐ 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

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

PROPERTY RIGHTS

- ☐ 820 Copyright
- ☐ 830 Patent
- ☐ 835 Patent - Abbreviated New Drug Application
- ☐ 840 Trademark
- ☐ 880 Defend Trade Secrets Act of 2016 (DTSA)

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
- ☐ 485 Telephone Consumer Protection Act (TCPA)
- ☐ 490 Cable/Sat TV
- ☐ 850 Securities/Commodities/ Exchange
- ☐ 890 Other Statutory Actions
- ☐ 891 Agricultural Arts
- ☐ 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

BANKRUPTCY

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

IMMIGRATION

- ☐ 462 Naturalization Application
- ☐ 463 Habeas Corpus – Alien Detainee (Prisoner Petition)
- ☐ 465 Other Immigration Actions

FORFEITURE/PENALTY

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

SOCIAL SECURITY

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

FEDERAL TAXES

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

V. ORIGIN *(Check **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 (Enter U.S. Civil Statute under which you are filing and write a brief statement of cause.)

Class Action Fairness Act, 28 U.S.C. § 1332(d)

VII. PREVIOUS BANKRUPTCY MATTERS (For nature of suit 422 and 423, enter the case number and judge for any associated bankruptcy matter previously adjudicated by a judge of this Court. Use a separate attachment if necessary.)

VIII. REQUESTED IN COMPLAINT:

☒ Check if this is a **class action** under Rule 23, F.R.C.V.P.

Demand $

CHECK Yes only if demanded in complaint:

Jury Demand: ☒ Yes ☐ No

IX. RELATED CASE(S) IF ANY *(See instructions):*

Judge Case Number

X. Is this a previously dismissed or remanded case?

☐ Yes ☐ No **If yes, Case #** **Name of Judge**

Date: 1/12/2026

Signature of Attorney of Record /s/ Jeff Ostrow

INSTRUCTIONS FOR ATTORNEYS COMPLETING CIVIL COVER SHEET FORM JS 44

Authority for Civil Cover Sheet

The ILND 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
(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
(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"
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
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.
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 statue.

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 pending cases, if any. If there are related pending cases, insert the docket numbers and the corresponding judge names for such cases.

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