IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF INDIANA

MARK KUHN, on behalf of himself and all others similarly situated, Plaintiff, v. **1ST SOURCE BANK** Defendant.	Case No.

CLASS ACTION COMPLAINT AND DEMAND FOR JURY TRIAL

Plaintiff Mark Kuhn ("Plaintiff"), individually and on behalf of all others similarly situated, brings this Class Action Complaint against Defendant 1st Source Bank ("1st Source") and alleges, upon personal knowledge as to his own actions and his counsel's investigations, and upon information and belief as to all other matters, as follows:

I. INTRODUCTION

1. Plaintiff brings this class action against 1st Source for its failure to properly safeguard and secure the personally identifiable information ("PII")[1] of 1st Source's current and former customers and other consumers for whom 1st Source performed services.

2. 1st Source Bank, a wholly owned subsidiary of 1st Source Corporation, offers commercial and consumer banking services, trust and wealth advisory services, and insurance to individual and business clients at 79 banking center locations in 18 counties in Indiana and

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

Michigan and Sarasota County in Florida. 1st Source Bank's Specialty Finance Group has 19 locations nationwide, and offers specialized financing services for construction equipment, new and pre-owned private and cargo aircraft, and various vehicle types (cars, trucks, vans) for fleet purposes.[2]

3. As of December 31, 2022, 1st Source had approximately 1,150 employees and consolidated total assets of $8.34 billion, total loans and leases of $6.01 billion, total deposits of $6.93 billion, and total shareholders' equity of $864.07 million.[3]

4. 1st Source is a sophisticated corporate entity and regularly maintains consumer information it knows to be sensitive. Moreover, it is aware of the consequences that would result for those consumers if the information were to be compromised and its corresponding obligation to protect against such compromise.

5. Prior to and through July 14, 2023, 1st Source, and in furtherance of its operations as a financial institution, obtained the PII of Plaintiff and Class Members, its customers, and transmitted that PII via the MOVEit file transfer software developed by Ipswitch, a subsidiary of Progress Software Corporation.

6. Sometime around June 1, 2023, an unauthorized external party affiliated with the notorious CL0P ransomware group breached exploited a vulnerability in the MOVEit software to infiltrate Defendant's computer network system and procure and exfiltrate massive amounts of PII belonging to 1st Source's clients and former clients, including the PII of Plaintiff and Class Members, including the full names, Social Security Numbers, driver's license or state identification card numbers, other government-issued identification numbers, and dates of birth

[2] 1st Source Corporation, Annual Report (Form 10-K) (2022) available at https://d18rn0p25nwr6d.cloudfront.net/CIK-0000034782/70024c42-9743-4b30-b925-90e1f260b8e6.pdf (last visited July 25, 2023).
[3] *Id.*

(the "Data Breach").

7. Despite having known about the Data Breach since at least June 1, 2023, notices were not sent to affected individuals until July 14, 2023.

8. Upon information and belief, 1st Source was targeted in the cyberattack due to the high volume of sensitive PII that it collected and maintained on its computer networks and/or systems and the high value of that information to cyber criminals in facilitating identity theft and fraud.

9. Per its Form 8-K filed July 10, 2023, 1st Source disclosed the Data Breach and admitted that an unauthorized third-party gained access to sensitive data of commercial and individual clients, including PII of individuals.[4]

10. On or around July 14, 2023, 1st Source began notifying various states Attorneys General of the Data Breach.

11. On or around July 14, 2023, 1st Source began notifying Plaintiff and Class Members of the Data Breach.

12. By obtaining, collecting, using, and deriving a benefit from the PII of Plaintiff and Class Members, 1st Source assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion. 1st Source admits that the unencrypted PII obtained by an unauthorized external party included full names, Social Security Numbers, driver's license or state identification card numbers, other government-issued identification numbers, and dates of birth.

13. The notorious ransomware gang, the Cl0p, has claimed responsibility for MOVEit

[4] 1st Source Corporation, Current Report (Form 8-K) (July 24, 2023) available at https://d18rn0p25nwr6d.cloudfront.net/CIK-0000034782/52f3f175-7405-4cc1-bbfb-22b16d232149.pdf (last visited July 25, 2023).

Transfer data-theft attack against 1st Source.[5]

14. The exposed PII of Plaintiff and Class Members was targeted due to its value on the dark web. Computer hackers, like the Cl0p, target and sell to criminals the unencrypted, unredacted PII that they exfiltrate from companies like 1st Source. Plaintiff and Class Members now face a present and continuing lifetime risk of: (i) identity theft, which is heightened here by the loss of Social Security numbers in conjunction with other sensitive information; and (ii) the sharing and detrimental use of their sensitive information over which they have now been deprived of control.

15. The PII was targeted and compromised due to 1st Source's negligent and/or careless acts and omissions and failure to protect the PII of Plaintiff and Class Members. In addition to 1st Source's failure to prevent the Data Breach, 1st Source has also purposefully maintained as secret the specific vulnerabilities and root causes of the breach and has not informed Plaintiff and Class Members of that information.

16. Plaintiff brings this action on behalf of all persons whose PII was compromised as a result of 1st Source's failures to: (i) adequately protect the PII of Plaintiff and Class Members; (ii) warn Plaintiff and Class Members of 1st Source's inadequate information security practices; and (iii) effectively secure hardware containing protected PII using reasonable and effective security procedures free of vulnerabilities and incidents. 1st Source's conduct amounts to negligence and violates federal and state statutes.

17. Plaintiff and Class Members have suffered injury as a result of 1st Source's conduct. These injuries include: (i) lost or diminished value of PII; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use

[5] https://www.bleepingcomputer.com/news/security/clop-ransomware-claims-responsibility-for-moveit-extortion-attacks/ (last visited July 25, 2023).

of their PII; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; (iv) the disclosure of their private information; (v) failure to receive the benefit of their bargains with 1st Source related to their financial products; (vi) nominal damages; (vii) the present and continuing risk to their PII, and damages in an amount equal to the cost of securing identity theft products to assisting in monitoring and protecting them from identity theft, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) may remain backed up in 1st Source's possession and is subject to further unauthorized disclosures so long as 1st Source fails to undertake appropriate and adequate measures to protect the PII.

18. 1st Source disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, or negligently failing to take and implement adequate and reasonable measures to ensure that the PII of Plaintiff and Class Members was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use. As a result, the PII of Plaintiff and Class Members was compromised through disclosure to an unknown and unauthorized third party. Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

II. PARTIES

Plaintiff Mark Kuhn

19. Plaintiff Mark Kuhn is an adult individual resident and citizen of California, where he intends to stay.

20. Plaintiff Kuhn is a former customer of 1st Source.

21. Plaintiff Kuhn received a Notice of Data Incident letter dated July 14, 2023, from 1st Source, indicating that his names, Social Security Number, driver's license or state identification card number, other government-issued identification number, and date of birth were impacted by the Data Breach.

Defendant 1st Source Bank

22. Defendant 1st Source is a for-profit corporation organized under the laws of the state of Indiana having its principal place of business in South Bend, Indiana.

23. 1st Source is a banking subsidiary of 1st Source Corporation, an Indiana corporation, and bank holding company, incorporated in 1971.

24. The true names and capacities of persons or entities, whether individual, corporate, associate, or otherwise, who may be responsible for some of the claims alleged herein are currently unknown to Plaintiff. Plaintiff will seek leave of court to amend this complaint to reflect the true names and capacities of other such responsible parties when their identities become known.

25. All of Plaintiff's claims stated herein are asserted against 1st Source and any of its owners, predecessors, successors, subsidiaries, agents and/or assigns.

III. JURISDICTION AND VENUE

26. This Court has subject matter and diversity jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount of controversy exceeds the sum or value of $5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one Class Member, including Plaintiff Kuhn, is a citizen of a state different from 1st Source to establish minimal diversity.

27. The Court has personal jurisdiction over 1st Source because, personally or through their agents, 1st Source operated, conducted, engaged in, or carried on a business or business

venture in Indiana and had offices in Indiana.

28. Venue is proper in this district under 28 U.S.C. §§ 1391(a)(1), 1391(b)(1), 1391(b)(2), and 1391(c)(2) as a substantial part of the events giving rise to the claims emanated from activities within this district, and 1st Source conducted substantial business in this district and reside in this district. Further, on information and belief, decisions regarding the management of the information security of Plaintiff's and Class Members' PII were made by 1st Source within this district. Moreover, it is believed that 1st Source maintained Plaintiff's and Class Members PII in the district, and the harm caused to Plaintiff and Class Members emanated from this district.

IV. FACTUAL ALLEGATIONS

Background

29. Plaintiff and Class Members, who are past and current clients of 1st Source, provided and entrusted 1st Source with sensitive and confidential information, including but not limited to includes names, email addresses, usernames, passwords, social security numbers, phone numbers, mailing addresses, financial information and history, employment information, drivers' license information, insurance information, marital status, and other personal and highly sensitive information a person is obligated to provide when applying for or requesting financial products. Because of this, 1st Source hosts a large repository of sensitive personal information for its customers. Much of the information Plaintiff and Class Members entrusted to 1st Source is static, does not change, and can be used to commit myriad financial crimes.

30. 1st Source's privacy policy, which is posted on its website, states that 1st Source collects personal information from customers when the customer applies for a loan, opens an account or provides account information, makes deposits or withdrawals, and applies for financing. 1st Source also collects additional personal information from credit bureaus, business affiliates,

and other companies.[6]

31. 1st Source acknowledges that it collects PII including customers' Social Security numbers and incomes, account balances and transaction histories, and credit histories and credit scores and shares that information for marketing purposes, for affiliates' everyday business purposes, joint marketing with affiliates, and for affiliates marketing purposes.[7]

32. As a condition of being a past or current customer of 1st Source, 1st Source required that Plaintiff and Class Members provide and entrust 1st Source with highly confidential PII.

33. 1st Source utilized the cloud hosting and file transfer service MOVEit provided by Progress Software to transfer and share Plaintiff's and Class Members' PII.

34. 1st Source shared the PII of Plaintiff and Class Members and stored the PII unencrypted and on its Internet-accessible network.

35. Plaintiff and Class Members relied on 1st Source to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. Plaintiff and Class Members value the integrity and confidentiality of their PII and demand security to safeguard their PII.

36. Sophisticated companies like 1st Source are aware of the different types of threat actors acting across the Internet and the type of criminal cybersecurity acts they employ for profit. Accordingly, it is imperative that 1st Source guard against those criminal exploits.

37. 1st Source knew that the PII they maintained was a target of data thieves and that they had a duty to protect Plaintiff's and Class Members' PII from unauthorized access.

38. 1st Source's Privacy Policy states, "To protect your personal information from

[6]https://web.archive.org/web/20230411153534/https://www.1stsource.com/app/uploads/2022/10/Privacy-1stsource_privacynotice_7-21_fillable.pdf (last visited July 25, 2023).
[7] *Id.*

unauthorized access and use, we use security measures that comply with federal law. These measures include computer safeguards, secured files, secured buildings, limited access of your personal financial information to only those employees who need it to perform their jobs, and confidentiality agreements with service providers."[8]

39. By obtaining, collecting, using, and profiting from Plaintiff's and Class Members' PII, 1st Source had a duty to adopt reasonable measures to protect Plaintiff's and Class Members' PII from involuntary disclosure to third parties. 1st Source collected, maintained, and profited from information that they knew to be private and sensitive, and were aware of the consequences to Plaintiff and Class Members if they failed to adequately protect that information. 1st Source breached their duty to Plaintiff and Class Members and allowed an attacker access to their systems without detection.

40. Plaintiff and Class Members relied on 1st Source to keep their PII confidential and securely maintained and to only make authorized disclosures of this PII, which 1st Source ultimately failed to do.

The Data Breach and Notice Letter

41. On or around July 14, 2023, 1st Source mailed Plaintiff and Class Members a letter entitled *Notice of Data Breach.*[9] The notice stated in part:

> **What Happened?**
>
> On June 1, 2023, we became aware of an alert issued by Progress Software – the company responsible for the MOVEit file transfer program – addressing a critical vulnerability affecting MOVEit, a solution used widely by businesses and governmental agencies, including 1st Source Bank, to securely transfer data. After becoming aware of the alert, we took immediate steps to patch our MOVEit system in accordance with Progress Software's instructions and conduct and internal assessment. 1st Source thereafter engaged leading,

[8] *Id.*

[9] Sample notice filed with the Office of the Maine Attorney General *available at* https://apps.web.maine.gov/online/aeviewer/ME/40/ecd3f2c2-8cdf-48cc-84f5-f3321ae41cd7/4f81b466-375c-4b44-bf4d-2c5b481f78ad/document.html (last visited July 25, 2023) (the "Notice Letter")

> independent cybersecurity experts to conduct a comprehensive investigation to determine the scope of potentially affected data. On June 24, 2023, we learned that your data was contained within a file that may have been acquired without authorization in connection with the MOVEit software vulnerability. Since that time, we have been collecting information needed to provide notice to potentially impacted individuals, including you.
>
> **What Information Was Involved?**
>
> The information potentially impacted in connection with this incident may have included your name as well as your Social Security number, driver's license or state identification card number, other government-issued identification number, and/or date of birth.

42. On or about July 14, 2023, 1st Source notified various state Attorneys General of the Data Breach and provided "sample" notices of the Data Breach. 1st Source reported the breach to the Office of the Maine Attorney General on or around July 14, 2023, and reported that 450,000 persons were affected by the Data Breach [10]

43. 1st Source admitted in the *Notice of Data Incident*, the letters to the Attorneys General, and the "sample" notices of the Data Breach that unauthorized third persons accessed and removed from their network systems sensitive information associated with 1st Source's customers, including: "your name, Social Security number, driver's license or state identification card number, other government-issued identification number, and/or date of birth.."[29] Much of this sensitive information is static, cannot change, and can be used to commit myriad financial crimes.

44. Upon information and belief, the accessed systems contained PII and that was accessible, unencrypted, unprotected, and vulnerable for acquisition and/or exfiltration by the unauthorized actor.

45. In response to the Data Breach, 1st Source claims it "took immediate steps to patch our MOVEit system in accordance with Progress Software's instructions and conduct an internal

[10] *Id.*

assessment."[11] However, the details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure a breach does not occur again have not been shared with Plaintiff and Class Members, who retain a vested interest in ensuring that their information remains protected.

46. 1st Source, upon information and belief, continues to utilize the MOVEit software and 1st Source has offered no assurance that its MOVEit software has been adequately enhanced so that it is not vulnerable to another data breach in the future.

47. Plaintiff's and Class Members' unencrypted PII has very likely been leaked onto the dark web, and/or may simply fall into the hands of companies that will use the detailed PII for targeted marketing without the approval of the affected current and former customers. Unauthorized individuals can access the PII of Plaintiff and Class Members now that it has been stolen.

48. 1st Source did not use reasonable security procedures and practices suitable or adequate to protect the sensitive, unencrypted information it was maintaining for consumers, causing the access and/or exfiltration of the PII of the affected individuals.

49. The targeted cyberattack by the CL0P ransomware group was expressly designed to gain access to and exfiltrate private and confidential data, including (among other things) the PII of banking customers like Plaintiff and Class Members.

50. In 2020, the CL0P ransomware group executed a targeted assault on Accellion's outdated file transfer appliance, acquiring massive quantities of data from over 100 affiliated companies. With a demand for a US$10 million ransom, they gradually divulged the stolen information, leading to breaches of privacy and data leaks.[12]

---

[11] *See Id.*

[12] https://techwireasia.com/2023/06/we-like-to-moveit-a-wake-up-call-for-cybersecurity/ (last visited July 25, 2023).

51. On February 23, 203, the CL0P ransomware gang exploited the Fortra GoAnywhere vulnerability, targeting global corporations, as well as city administrations and regional governments.[13]

52. 1st Source knew or should have known that its computer systems were a target for cybersecurity attacks, including attacks involving data theft, because warnings were readily available and accessible via the internet. In addition to articles in the public press about the extensive number of data breaches affecting companies throughout all industries, including the financial industry, governmental agencies have constantly sent and published notices of the need for companies, including those in the financial industry to carefully safeguard the sensitive and valuable information collected from consumers.

53. This readily available and accessible information confirms that, prior to the Data Breach, 1st Source knew or should have known that (i) unauthorized actors were targeting companies such as 1st Source (ii) unauthorized actors were aggressive in their pursuit of companies such as 1st Source, (iii) unauthorized actors were leaking corporate information on dark web portals, and (iv) unauthorized actors' tactics included threatening to release stolen data.

54. Given 1st Source's knowledge that the sensitive information it maintained would be targeted by hackers, 1st Source had a duty to institute appropriate data security procedures to guard against this threat.

55. In light of the information readily available and accessible on the internet before the Data Breach, 1st Source, having elected to share the unencrypted PII of consumers with third party affiliate and having elected to store that PII and other similar PII from other entities in an Internet-accessible environment, had reason to be on guard for the targeting and exfiltration of the

[13] https://www.bleepingcomputer.com/news/security/fortra-shares-findings-on-goanywhere-mft-zero-day-attacks/

PII at issue here. 1st Source should have been particularly on guard against such an attack as a result of their foreknowledge as demonstrated in their public representations.

56. Prior to the Data Breach, 1st Source knew or should have known that there was a foreseeable risk that Plaintiff's and Class Members' PII could be accessed, exfiltrated, and published as the result of a cyberattack.

57. Prior to the Data Breach, 1st Source knew or should have known that it should have encrypted the PII to protect against their publication and misuse in the event of a cyberattack.

58. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' PII, 1st Source assumed legal and equitable duties and knew, or should have known, that it was responsible for protecting Plaintiff's and Class Members' PII from unauthorized disclosure.

Data Breaches are Preventable

59. To prevent and detect cyber-attacks and/or ransomware attacks 1st Source could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.

- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.
- Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment.
- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[14]

60. To prevent and detect cyber-attacks or ransomware attacks 1st Source could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Secure internet-facing assets

- Apply latest security updates
- Use threat and vulnerability management
- Perform regular audit; remove privileged credentials;

[14]https://www.meritalk.com/articles/fbi-high-impact-ransomware-attacks-threaten-u-s-businesses-and-organizations/ (last visited July 25, 2023).

Thoroughly investigate and remediate alerts

- Prioritize and treat commodity malware infections as potential full compromise;

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;

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[15]

61. Given that 1st Source were storing the PII of so many individuals, 1st Source could and should have implemented all the above measures to prevent and detect cyberattacks, and their failure to do so was negligent if not reckless.

62. The occurrence of the Data Breach evidences that 1st Source failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach

[15] *See* Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), *available at:* https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/ (last visited July 25, 2023).

and the exposure of the PII of Plaintiff and Class Members.

1st Source Failed to Comply with FTC Guidelines

63. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which 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.

64. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. 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.[16]

65. The 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.[17]

66. The FTC further recommends that companies not maintain PII 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.

[16] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016). Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited July 25, 2023).
[17] *Id*.

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

68. These FTC enforcement actions include actions against companies like 1st Source.

69. 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 1st Source, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of 1st Source's duty in this regard.

70. 1st Source failed to properly implement basic data security practices.

71. 1st Source's failure to employ reasonable and appropriate measures to protect against unauthorized access to customers' PII or to comply with applicable industry standards constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

72. Upon information and belief, 1st Source were at all times fully aware of their obligation to protect the PII of their customers and clients' customers, 1st Source were also aware of the significant repercussions that would result from their failure to do so. Accordingly, 1st Source's conduct was particularly unreasonable given the nature and amount of PII they obtained and stored and the foreseeable consequences of the immense damage that would result to Plaintiff and the Class.

1st Source Failed to Follow Industry Standards

73. As noted above, experts studying cyber security routinely identify entities in possession of PII as being particularly vulnerable to cyberattacks because of the value of the PII which they collect and maintain.

74. Several best practices have been identified that, at a minimum, should be implemented by companies in possession of PII like 1st Source, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data and limiting which customers can access sensitive data. 1st Source failed to follow these industry best practices, including a failure to implement multi-factor authentication.

75. Other best cybersecurity practices that are standard for companies in possession of PII include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points. 1st Source failed to follow these cybersecurity best practices, including failure to train staff.

76. 1st Source failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

77. These foregoing frameworks are existing and applicable industry standards for

companies in possession of PII, and upon information and belief, 1st Source failed to comply with at least one—or all—of these accepted standards, thereby opening the door to the threat actor and causing the Data Breach.

1st Source failed to comply with the Gramm-Leach-Bliley Act

78. 1st Source offers consumers financial products or services like loans and loans servicing and are therefore subject to the Gramm-Leach-Bliley Act ("GLBA").

79. 1st Source collect nonpublic personal information, as defined by 15 U.S.C. § 6809(4)(A), 16 C.F.R. § 313.3(n) and 12 C.F.R. § 1016.3(p)(1). Accordingly, during the relevant time period 1st Source were subject to the requirements of the GLBA, 15 U.S.C. §§ 6801.1 et seq., and are subject to numerous rules and regulations promulgated on the GLBA Statutes. The GLBA Privacy Rule became effective on July 1, 2001. See 16 C.F.R. Part 313. Since the enactment of the Dodd-Frank Act on July 21, 2010, the Consumer Financial Protection Bureau ("CFPB") became responsible for implementing the Privacy Rule. In December 2011, the CFPB restated the implementing regulations in an interim final rule that established the Privacy of Consumer Financial Information, Regulation P, 12 C.F.R. § 1016 ("Regulation P"), with the final version becoming effective on October 28, 2014.

80. Accordingly, 1st Source's conduct is governed by the Privacy Rule prior to December 30, 2011, and by Regulation P after that date.

81. Both the Privacy Rule and Regulation P require financial institutions to provide customers with an initial and annual privacy notice. These privacy notices must be "clear and conspicuous."16 C.F.R. §§ 313.4 and 313.5; 12 C.F.R. §§ 1016.4 and 1016.5. "Clear and conspicuous means that a notice is reasonably understandable and designed to call attention to the nature and significance of the information in the notice." 16 C.F.R. § 313.3(b)(1); 12 C.F.R. §

1016.3(b)(1). These privacy notices must "accurately reflect[] [the financial institution's] privacy policies and practices." 16 C.F.R. § 313.4 and 313.5; 12 C.F.R. §§ 1016.4 and 1016.5. They must include specified elements, including the categories of nonpublic personal information the financial institution collects and discloses, the categories of third parties to whom the financial institution discloses the information, and the financial institution's security and confidentiality policies and practices for nonpublic personal information. 16 C.F.R. § 313.6; 12 C.F.R. § 1016.6. These privacy notices must be provided "so that each consumer can reasonably be expected to receive actual notice." 16 C.F.R. § 313.9; 12 C.F.R. § 1016.9. As alleged herein, 1st Source violated the Privacy Rule and Regulation P.

82. Upon information and belief, 1st Source failed to provide annual privacy notices to customers after the customer relationship ended, despite retaining these customers' PII and storing and/or sharing that PII on its network.

83. 1st Source failed to adequately inform its customers that it was storing and/or sharing, or would store and/or share, the customers' PII on its inadequately secured network and would do so after the customer relationship ended.

84. The Safeguards Rule, which implements Section 501(b) of the GLBA,15 U.S.C. § 6801(b), requires institutions to protect the security, confidentiality, and integrity of customer information by developing a comprehensive written information security program that contains reasonable administrative, technical, and physical safeguards, including: (1) designating one or more employees to coordinate the information security program; (2) identifying reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information, and assessing the sufficiency of any safeguards in place to control those risks; (3) designing and implementing information safeguards to control the risks identified through risk

assessment, and regularly testing or otherwise monitoring the effectiveness of the safeguards' key controls, systems, and procedures; (4) overseeing service providers and requiring them by contract to protect the security and confidentiality of customer information; and (5) evaluating and adjusting the information security program in light of the results of testing and monitoring, changes to the business operation, and other relevant circumstances. 16 C.F.R. §§ 314.3 and 314.4. As alleged herein, 1st Source violated the Safeguard Rule.

85. 1st Source failed to assess reasonably foreseeable risks to the security, confidentiality, and integrity of PII in its custody or control.

86. 1st Source 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.

87. 1st Source failed to adequately oversee service providers.

88. 1st Source failed to evaluate and adjust its information security program in light of the results of testing and monitoring, changes to the business operation, and other relevant circumstances.

The Data Breach was Foreseeable

89. 1st Source's data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches targeting entities that collect and store PII, like 1st Source, preceding the date of the breach.

90. Data breaches, including those perpetrated against financial entities that store PII in their systems, have become widespread.

91. 1st Source knew or should have known that these attacks were common and foreseeable. In 2022, there were 1,802 data breaches, nearly eclipsing 2021's record wherein 1,862

data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.[18] The 330 reported breaches reported in 2021 exposed nearly 30 million sensitive records (28,045,658), compared to only 306 breaches that exposed nearly 10 million sensitive records (9,700,238) in 2020.[19]

92. In light of recent high profile data breaches at other industry leading companies, including, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), 1st Source knew or should have known that their electronic records would be targeted by cybercriminals.

93. Indeed, cyberattacks have become so notorious that the FBI and U.S. Secret Service regularly issue warnings to potential targets, so they are aware of and take appropriate measures to prepare for and are able to thwart such an attack.

94. Despite the prevalence of public announcements of data breach and data security compromises, 1st Source failed to take appropriate steps to protect the PII of Plaintiff and Class Members from being compromised.

Plaintiff and Class Members are under a Present and Continuing Risk of Identity Theft and Fraud

95. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[20] The FTC describes "identifying

[18] *See* 2021 Data Breach Annual Report (ITRC, Jan. 2022) (available at https://notified.idtheftcenter.org/s/), at 6 (last visited July 25, 2023).
[19] See Data Breaches Hit Lots More People in 2022 (Jan. 25, 2023) https://www.cnet.com/tech/services-and-software/data-breaches-hit-lots-more-people-in-2022/ (last visited July 25, 2023).
[20] 17 C.F.R. § 248.201 (2013).

information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[21]

96. The FTC recommends that identity theft victims take several steps to protect their personal health and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (and to consider an extended fraud alert that lasts for seven years if identity theft occurs), 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.[22]

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

98. PII provided by consumers to a financial institution, typically provided under penalty of 18 U.S.C. § 1344, is accurate and of great value to hackers and cyber criminals, and the data stolen in the Data Breach has been used and will continue to be used in a variety of sordid ways for criminals to exploit Plaintiff and Class Members and to profit off their misfortune.

99. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

---

[21] *Id.*

[22] *Identity Theft Recovery Steps*, FTC, https://www.identitytheft.gov/Steps (last visited July 25, 2023). [https://perma.cc/ME45-5N3A].

100. The fraudulent activity resulting from the Data Breach may not come to light for years.

101. There may be a time lag between when harm occurs versus when it is discovered, and also between when the PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data has been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[23]

102. One such example of criminals piecing together bits and pieces of compromised PII for profit is the development of "Fullz" packages.[24]

103. With "Fullz" packages, cyber-criminals can cross-reference two sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals.

104. The development of "Fullz" packages means here that the stolen PII from the Data Breach can easily be used to link and identify it to Plaintiff's and Class Members' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII

---

[23] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* https://www.gao.gov/assets/gao-07-737.pdf (last visited July 25, 2023).

[24] "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made from those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See*, *e.g.*, Brian Krebs, *Medical Records for Sale in Underground Stolen from Texas Life Insurance Firm*, Krebs on Security (Sep. 18, 2014), https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-firm/ (last visited July 25, 2023).

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. Moreover, because much of the information at issue here includes immutable data like Social Security numbers, names, and, for all practical purposes, home addresses, Plaintiff's and Class Members' PII can be used to victimize them for the remainder of their lives.

105. The existence and prevalence of "Fullz" packages means that the PII stolen from the data breach can easily be linked to the unregulated data (like phone numbers and emails) of Plaintiff and the other Class Members. And because the criminals here have either the full or the last four numbers of Plaintiff's and Class Members' Social Security numbers, they can easily obtain the last four numbers, which are often used as identifiers, through techniques like social engineering.

106. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate and trick individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails. Data breaches are often the starting point for these additional targeted attacks on the victims.

107. Thus, even if certain information (such as emails or telephone numbers) was not stolen in the data breach, criminals can still easily create a comprehensive "Fullz" package.

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

109. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of 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.[25]

110. What is 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.

111. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "The 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."[26]

112. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts, although cyber criminals can still use this information to develop synthetic identities and can engage if financial crimes. The information compromised in this Data Breach is impossible to "close" and difficult,

---

[25] Social Security Administration, *Identity Theft and Your Social Security Number*, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited July 25, 2023).

[26] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), *available at*: http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft (last visited July 25, 2023).

if not impossible, to change.

113. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market." [27]

114. Plaintiff and Class Members now face a lifetime of constant surveillance of their financial and personal records, monitoring, and loss of rights. Plaintiff and Class Members are incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

115. The ramifications of 1st Source's failure to keep secure the PII of Plaintiff and Class Members are long lasting and severe. Once PII is stolen, particularly Social Security numbers, fraudulent use of that information and damage to victims may continue for years.

Value of Personal Identifiable Information

116. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200[28], and bank details have a price range of $50 to $200.[29] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web. Criminals can also purchase access to entire company data breaches from $900 to $4,500.[30]

---

[27] Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), *available at*: https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited July 25, 2023).

[28] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last visited July 25, 2023).

[29] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last accessed June 14, 2023).

[30] *In the Dark*, VPN Overview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last visited July 25, 2023).

117. An active and robust legitimate marketplace for PII exists. In 2019, the data brokering industry was worth roughly $200 billion.[31]

118. 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.[32],[33]

119. Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.[34]

120. Conversely sensitive PII can sell for as much as $363 per record on the dark web according to the Infosec Institute.[35]

121. As a result of the Data Breach, Plaintiff's and Class Members' PII, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its compromise and unauthorized release. However, this transfer of value occurred without any consideration paid to Plaintiff or Class Members for their property, resulting in an economic loss. Moreover, the PII is now readily available, and the rarity of the Data has been lost, thereby causing additional loss of value.

122. 1st Source was, or should have been, fully aware of the unique type and the significant volume of data contained in the PII that 1st Source collected and maintained amounting to hundreds of thousands of individuals' detailed, personal information and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

---

[31] Shadowy data brokers make the most of their invisibility cloak, Los Angeles Times, Nov. 5, 2019, available at https://www.latimes.com/business/story/2019-11-05/column-data-brokers (last visited July 25, 2023).
[32] *See* https://datacoup.com.
[33] *See* https://digi.me/what-is-digime/.
[34] Nielsen Computer & Mobile Panel, Frequently Asked Questions, available at https://computermobilepanel.nielsen.com/ui/US/en/faqen.html (last visited June 14, 2023)
[35] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/ (last visited July 25, 2023).

123. To date, 1st Source has offered Plaintiff and Class Members only one year of credit identity monitoring services. The offered service is inadequate to protect Plaintiff and Class Members from the threats they face for the remainder of their lives in light of the PII at issue here.

124. That 1st Source is encouraging Plaintiff and Class Members to enroll in credit monitoring and identity theft restoration services is an acknowledgment that the impacted individuals' PII was acquired, thereby subjecting Plaintiff and Class Members to a substantial and imminent threat of fraud and identity theft.

125. The injuries to Plaintiff and Class Members were directly and proximately caused by 1st Source's failure to implement or maintain adequate data security measures for the PII of Plaintiff and Class Members.

Plaintiff Kuhn's Experience

126. Plaintiff Kuhn was a customer of 1st Source approximately 20 years ago. As a condition of using 1st Source's financial services, Plaintiff Kuhn was required to provide his PII to 1st Source which was then entered by 1st Source into its database that has been maintained by 1st Source.

127. Plaintiff Kuhn greatly values his privacy and PII. Prior to the Data Breach, Plaintiff Kuhn took reasonable steps to maintain the confidentiality of his PII.

128. Plaintiff Kuhn received a letter dated July 14, 2023, from 1st Source concerning the Data Breach. The letter stated that unauthorized actors gained access to files containing 1st Source's sensitive PII by exploiting a critical vulnerability affecting 1st Source's data transfer software known as MOVEit.

129. The compromised files contained Plaintiff Kuhn's name, Social Security number, driver's license or state identification card number, other government-issued identification

number, and date of birth.

130. Since learning of the Data Breach, Plaintiff Kuhn has spent additional time reviewing his bank statements and credit cards. Since the date of the breach, he has spent several hours reviewing his accounts and credit reports. Plaintiff Kuhn has also spent valuable time signing up for the credit monitoring service offered by Kroll.

131. Plaintiff Kuhn has experienced actual fraud when his wife's American Express card, where he is the primary card holder, was improperly accessed and suffered unauthorized charges. The American Express card was cancelled as a result of the fraud. It took approximately one week for a new card to be issued.

132. The Data Breach has caused Plaintiff Kuhn to suffer fear, anxiety, and stress, which has been compounded by the fact that 1st Source has not been forthright with information about the Data Breach.

133. Plaintiff Kuhn plans to take additional time-consuming, necessary steps to help mitigate the harm caused by the Data Breach, including continually reviewing his depository, credit, and other accounts for any unauthorized activity.

134. Additionally, Plaintiff Kuhn is very careful about sharing his PII. He has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

135. Plaintiff Kuhn stores any documents containing his PII in a safe and secure location or destroys the documents. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

136. Plaintiff Kuhn has a continuing interest in ensuring that his PII, which, upon information and belief, remains in 1st Source's possession, is protected and safeguarded from future data breaches.

V. CLASS ALLEGATIONS

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

138. The Class that Plaintiff seeks to represent is preliminarily defined as follows:

> All individuals residing in the United States whose PII was accessed or exfiltrated during the Data Breach announced by Defendant 1st Source Bank in July 2023 (the "Class").

139. 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 have a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

140. Plaintiff reserves the right to modify or amend the definition of the proposed classes before the Court determines whether certification is appropriate.

141. Numerosity, Fed R. Civ. P. 23(a)(1): The Class is so numerous that joinder of all members is impracticable. Defendant has identified thousands of individuals whose PII was compromised in the Data Breach, and the Class is apparently identifiable within Defendant's records. Defendant notified the Office of the Maine Attorney General that 450,000 persons were affected by the Data Breach.[36]

142. Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3): Questions of law and fact

[36] https://apps.web.maine.gov/online/aeviewer/ME/40/ecd3f2c2-8cdf-48cc-84f5-f3321ae41cd7.shtml (last visited July 25, 2023).

common to the Class exist and predominate over any questions affecting only individual Class Members. These include:

a. Whether and to what extent Defendant had duties to protect the PII of Plaintiff and Class Members;

b. Whether Defendant had duties not to disclose the PII of Plaintiff and Class Members to unauthorized third parties;

c. Whether Defendant had duties not to use the PII of Plaintiff and Class Members for non-business purposes;

d. Whether Defendant failed to adequately safeguard the PII of Plaintiff and Class Members;

e. When Defendant actually learned of the Data Breach;

f. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their PII had been compromised;

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

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

i. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

j. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Plaintiff and Class Members;

k. Whether Plaintiff and Class Members are entitled to actual, consequential, and/or

nominal damages as a result of Defendant's wrongful conduct;

l. Whether Plaintiff and Class Members are entitled to restitution as a result of Defendant's wrongful conduct; and

m. 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.

143. Typicality, Fed. R. Civ. P. 23(a)(3): Plaintiff's claims are typical of those of other Class Members because all had their PII compromised as a result of the Data Breach, due to Defendant's misfeasance.

144. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendant has 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 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.

145. Adequacy, Fed. R. Civ. P. 23(a)(4): Plaintiff will fairly and adequately represent and protect the interests of the Class in that Plaintiff has no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiff seeks no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages they have suffered are typical of other Class Members. Plaintiff has retained counsel experienced in complex class action litigation, and Plaintiff intends to prosecute this action vigorously.

146. Superiority and Manageability, Fed. R. Civ. P. 23(b)(3): 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.

147. 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 they 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.

148. 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 demonstrate that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

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

150. Unless a Class-wide injunction is issued, Defendant may continue in their failure to properly secure the PII 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.

151. Further, Defendant has acted or refused to act on grounds generally applicable to the Classes and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

152. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant owed legal duties to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;
b. Whether Defendant breached legal duties to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;
c. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;
d. Whether an implied contract existed between Defendant on the one hand, and Plaintiff and Class Members on the other, and the terms of that implied contract;
e. Whether Defendant breached the implied contract;

f. Whether Defendant adequately and accurately informed Plaintiff and Class Members that their PII had been compromised;

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

h. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Plaintiff and Class Members; and,

i. Whether Class Members are entitled to actual, consequential, and/or nominal damages, and/or injunctive relief as a result of Defendant's wrongful conduct.

Count I
Negligence
(On Behalf of Plaintiff and the Class)

153. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 152.

154. Plaintiff and Class Members were required to submit non-public PII as a condition of obtaining products and/or services from 1st Source or one of 1st Source's client companies.

155. Plaintiff and the Class Members entrusted their PII to 1st Source with the understanding that 1st Source would safeguard their information and delete it once it was no longer required to retain it after the end of the consumer relationship.

156. 1st Source had a duty to employ reasonable security measures and otherwise protect the PII of Plaintiff and Class Members.

157. 1st Source had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of

failing to use reasonable measures to protect confidential data.

158. 1st Source had full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and Class Members could and would suffer if the PII were wrongfully disclosed.

159. By assuming the responsibility to collect and store this data, and in fact doing so, and sharing it and using it for commercial gain, 1st Source had a duty of care to use reasonable means to secure and safeguard their computer property—and Class Members' PII held within it—to prevent disclosure of the information, and to safeguard the information from theft. 1st Source's duty included a responsibility to implement processes by which they could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

160. 1st Source's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because 1st Source is bound by industry standards to protect confidential PII.

161. 1st Source breached its duties, and thus were negligent, by failing to use reasonable measures to protect Class Members' PII. The specific negligent acts and omissions committed by 1st Source include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' PII;

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

c. Failing to periodically ensure that their email system had plans in place to maintain reasonable data security safeguards; and

d. Allowing unauthorized access to Class Members' PII.

162. It was foreseeable that 1st Source's failure to use reasonable measures to protect

Class Members' PII would result in injury to Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the industry.

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

164. Plaintiff and Class Members were the foreseeable and probable victims of any inadequate security practices and procedures. 1st Source knew or should have known of the inherent risks in collecting and storing the PII of Plaintiff and Class Members, the critical importance of providing adequate security of that PII, and the necessity for encrypting PII stored in an Internet-accessible environment.

165. 1st Source knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the PII of Plaintiff and Class Members involved an unreasonable risk of harm to Plaintiff and Class Members, even if the harm occurred through the criminal acts of a third party.

166. Plaintiff and Class Members had no ability to protect their PII that was in, and possibly remains in, 1st Source's possession.

167. 1st Source was in an exclusive position to protect against the harm suffered by Plaintiff and Class Members as a result of the Data Breach.

168. There is a temporal and close causal connection between 1st Source's failure to implement security measures to protect the PII and the harm suffered, or risk of imminent harm suffered by Plaintiff and Class Members.

169. As a result of 1st Source's negligence, Plaintiff and the Class Members have suffered and will continue to suffer damages and injury including, but not limited to: (i) lost or

diminished value of PII; (ii) invasion of privacy; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; (iv) loss of benefit of the bargain; and (v) the present and continuing risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remain backed up in 1st Source's possession and is subject to further unauthorized disclosures so long as 1st Source fail to undertake appropriate and adequate measures to protect the PII.

170. Plaintiff and Class Members are entitled to nominal, compensatory, and consequential damages suffered as a result of the Data Breach as well as any other relief allowed by law.

171. Plaintiff and Class Members are also entitled to injunctive relief requiring 1st Source to, e.g., (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

Count II
Breach of Implied Contract
(On Behalf of Plaintiff and the Class)

172. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 152.

173. 1st Source acquired and maintained the PII of Plaintiff and Class Members, including name, Social Security number, driver's license or state identification card number, other government-issued identification number, and date of birth.

174. At the time 1st Source acquired the PII of Plaintiff and Class Members, there was a meeting of the minds and a mutual understanding that 1st Source would safeguard the PII and

not take unjustified risks when storing the PII.

175. Plaintiff and Class Members would not have entrusted their PII to had they known that 1st Source would make the PII internet-accessible, not encrypt sensitive data elements such as Social Security numbers, and not delete the PII that 1st Source no longer had a reasonable need to maintain.

176. Prior to the Data Breach, 1st Source each published a Privacy Policy, agreeing to protect and keep private financial information of Plaintiff and Class Members.

177. 1st Source further promised to comply with industry standards and to ensure that Plaintiff's and Class Members' PII would remain protected.

178. Implicit in the agreements between Plaintiff and Class Members and 1st Source to directly and indirectly provide PII, was the latter's obligation to: (a) use such PII for business purposes only, (b) take reasonable steps to safeguard that PII, (c) prevent unauthorized disclosures of the PII, (d) provide Plaintiff and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their PII, (e) reasonably safeguard and protect the PII of Plaintiff and Class Members from unauthorized disclosure or uses, and (f) retain the PII only under conditions that kept such information secure and confidential.

179. In collecting and maintaining the PII of Plaintiff and Class Members and publishing their privacy policies, 1st Source entered into implied contracts with Plaintiff and Class Members requiring 1st Source to protect and keep secure the PII of Plaintiff and Class Members.

180. Plaintiff and Class Members fully performed their obligations under the contracts with 1st Source.

181. 1st Source breached the contracts it made with Plaintiff and Class Members by failing to protect and keep private financial information of Plaintiff and Class Members, including

failing to (i) encrypt or tokenize the sensitive PII of Plaintiff and Class Members, (ii) delete such PII that 1st Source no longer had reason to maintain, (iii) eliminate the potential accessibility of the PII from the internet where such accessibility was not justified, and (iv) otherwise review and improve the security of the network system that contained such PII.

182. As a direct and proximate result of 1st Source's above-described breach of implied contract, Plaintiff and Class Members have suffered (and will continue to suffer): ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; additional time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, credit freezes; decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

183. As a direct and proximate result of 1st Source's breach of contract, Plaintiff and Class Members are at a present and continuing risk of identity theft or fraud.

184. As a direct and proximate result of 1st Source's breach of contract, Plaintiff and Class Members are entitled to and demand actual, consequential, and nominal damages and injunctive relief, to be determined at trial.

Count III
Breach of Fiduciary Duty
(On Behalf of Plaintiff and the Class)

185. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 152.

186. A relationship existed between Plaintiff and Class Members and 1st Source in

which Plaintiff and Class Members put their trust in 1st Source to protect the private information of Plaintiff and Class Members and 1st Source accepted that trust.

187. 1st Source breached the fiduciary duties that they owed to Plaintiff and Class Members by failing to act with the utmost good faith, fairness, and honesty, failing to act with the highest and finest loyalty, and failing to protect the private information of Plaintiff and Class Members.

188. 1st Source's breach of fiduciary duty was a legal cause of damage to Plaintiff and Class Members.

189. But for 1st Source's breach of fiduciary duty, the damage to Plaintiff and Class Members would not have occurred.

190. 1st Source's breach of fiduciary duty contributed substantially to producing the damage to Plaintiff and Class Members.

191. As a direct and proximate result of 1st Source's breach of fiduciary duty, Plaintiff and Class Members are entitled to and demand actual, consequential, and nominal damages and injunctive relief.

Count IV
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

192. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 152.

193. When Plaintiff and Class Members paid for services and provided their PII to 1st Source, they did so on the mutual understanding and expectation that 1st Source would use a portion of those payments, or revenue derived from the use of their PII, to adequately fund data security practices.

194. Upon information and belief, 1st Source funds their data security measures entirely from their general revenues, including payments made by or on behalf of Plaintiff and Class Members and revenue derived from the PII provided by Plaintiff and Class Members.

195. Upon information and belief, 1st Source funds its data security measures entirely from their general revenues, including payments made by or on behalf of Plaintiff and Class Members and revenue derived from the PII provided by Plaintiff and Class Members.

196. As such, a portion of the payments made by or on behalf of Plaintiff and Class Members, or the revenue derived from their PII, is to be used by 1st Source to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to 1st Source.

197. 1st Source enriched itself by saving the costs they reasonably should have expended on data security measures to secure Plaintiff's and Class Members' PII and instead directing those funds to their own profits. Instead of providing a reasonable level of security that would have prevented the hacking incident, 1st Source instead calculated to increase its own profits at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of 1st Source's decision to prioritize its own profits over the requisite security.

198. 1st Source knew that Plaintiff and Class Members conferred a benefit which 1st Source accepted. 1st Source profited from these transactions and used the PII of Plaintiff and Class Members for business purposes.

199. For years and continuing to today, 1st Source's business model has depended upon their use of consumers' PII. Trust and confidence are critical and central to the services provided by 1st Source in the financial industry. Unbeknownst to Plaintiff and Class Members, however,

1st Source did not secure, safeguard, or protect its customers' data and employed deficient security procedures and protocols to prevent unauthorized access to customers' PII. 1st Source's deficiencies described herein were contrary to its security messaging.

200. Plaintiff and Class Members received services from 1st Source, and 1st Source were provided with, and allowed to collect and store, their PII on the mistaken belief that 1st Source complied with their duties to safeguard and protect its customers' and employees' PII.

201. Upon information and belief, putting their short-term profit ahead of safeguarding PII, and unbeknownst to Plaintiff and Class Members, 1st Source knowingly sacrificed data security to save money at their expense and to their detriment.

202. Upon information and belief, 1st Source knew that the manner in which they maintained and transmitted customer PII violated industry standards and their fundamental duties to Plaintiff and Class Members by neglecting well accepted security measures to ensure confidential information was not accessible to unauthorized access. 1st Source had knowledge of methods for designing safeguards against unauthorized access and eliminating the threat of exploitation, but it did not use such methods.

203. 1st Source had within their exclusive knowledge, and never disclosed, that they had failed to safeguard and protect Plaintiff's and Class Members' PII. This information was not available to Plaintiff, Class Members, or the public at large.

204. 1st Source also knew that Plaintiff and Class Members expected security against known risks and that they were required to adhere to state and federal standards for the protection of confidential personally identifying, financial, and other personal information.

205. Plaintiff and Class Members did not expect that 1st Source would knowingly insecurely maintain and hold their PII when that data was no longer needed to facilitate a business

transaction or other legitimate business reason. Likewise, Plaintiff and Class Members did not know or expect that 1st Source would employ substantially deficient data security systems and fail to undertake any required monitoring or supervision of the entrusted PII.

206. Had Plaintiff and Class Members known about 1st Source's deficiencies and efforts to hide their ineffective and substandard data security systems, Plaintiff and Class Members would not have entered into business dealings with 1st Source.

207. By withholding the facts concerning the defective security and protection of customer PII, 1st Source put its own interests ahead of the very customers who placed their trust and confidence in 1st Source and benefitted itself to the detriment of Plaintiff and Class Members.

208. It would be inequitable, unfair, and unjust for 1st Source to retain these wrongfully obtained fees and benefits. 1st Source's retention of wrongfully obtained monies would violate fundamental principles of justice, equity, and good conscience.

209. Plaintiff and Class Members have no adequate remedy at law.

210. Plaintiff and each Class Member are each entitled to restitution and non-restitutionary disgorgement in the amount by which 1st Source was unjustly enriched, to be determined at trial.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and the Class Members request judgment against 1st Source and that the Court grant the following:

A. For an Order certifying the Class and appointing Plaintiff and his Counsel to represent the Class;

B. For equitable relief enjoining 1st Source from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the PII of

Plaintiff and Class Members and from refusing to issue prompt, complete, any accurate disclosures to Plaintiff and Class Members;

C. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:

i. prohibiting 1st Source from engaging in the wrongful and unlawful acts described herein;

ii. requiring 1st Source to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring 1st Source to delete, destroy, and purge the personal identifying information of Plaintiff and Class Members unless 1st Source can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

iv. requiring 1st Source to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiff and Class Members;

v. prohibiting 1st Source from maintaining the PII of Plaintiff and Class Members on a cloud-based database;

vi. requiring 1st Source to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on 1st

Source's systems on a periodic basis, and ordering 1st Source to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring 1st Source to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring 1st Source to audit, test, and train their security personnel regarding any new or modified procedures;

ix. requiring 1st Source to segment data by, among other things, creating firewalls and access controls so that if one area of 1st Source's network is compromised, hackers cannot gain access to other portions of 1st Source's systems;

x. requiring 1st Source to conduct regular database scanning and securing checks;

xi. requiring 1st Source to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;

xii. requiring 1st Source to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. requiring 1st Source to implement a system of tests to assess their respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employee's

compliance with 1st Source's policies, programs, and systems for protecting personal identifying information;

xiv. requiring 1st Source to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor its information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring 1st Source to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. requiring 1st Source to implement logging and monitoring programs sufficient to track traffic to and from 1st Source's servers; and for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate 1st Source's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

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

E. For an award of attorneys' fees, costs, and litigation expenses as allowed by law;

F. For prejudgment interest on all amounts awarded; and

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

H.

DEMAND FOR A JURY TRIAL

Plaintiff herby demands that this matter be tried before a jury.

Date: July 25, 2023

Respectfully Submitted,

/s/ Gary M. Klinger
Gary M. Klinger
Milberg Coleman Bryson
Phillips Grossman, PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Telephone: (866) 252-0878
gklinger@milberg.com

Terence R. Coates*
tcoates@msdlegal.com
Justin C. Walker*
jwalker@msdlegal.com
Markovits, Stock & DeMarco, LLC
119 East Court Street, Suite 530
Cincinnati, OH 45202
Telephone: (513) 651-3700

* Pro Hac Vice Forthcoming

Counsel for Plaintiff and the Putative Class

JS 44 (Rev. 07/16)

CIVIL COVER SHEET

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

I. (a) PLAINTIFFS

MARK KUHN, on behalf of himself and all others similarly situated,

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

(c) Attorneys *(Firm Name, Address, and Telephone Number)*
Gary M. Klinger, MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN PLLC, 227 W. Monroe Street, Suite 2100, Chicago, IL 60606; (866) 252-0878

DEFENDANTS

1ST SOURCE BANK

County of Residence of First Listed Defendant St. Joseph County, Indiana
(IN U.S. PLAINTIFF CASES ONLY)

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

Attorneys *(If Known)*

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

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

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

(For Diversity Cases Only)

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

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

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

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

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

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

PRISONER PETITIONS

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

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

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

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

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

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

PROPERTY RIGHTS
- ❒ 820 Copyrights
- ❒ 830 Patent
- ❒ 840 Trademark

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

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

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

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

☒ 1 Original Proceeding ❒ 2 Removed from State Court ❒ 3 Remanded from Appellate Court ❒ 4 Reinstated or Reopened ❒ 5 Transferred from Another District *(specify)* ❒ 6 Multidistrict Litigation - Transfer ❒ 8 Multidistrict Litigation - Direct File

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing ***(Do not cite jurisdictional statutes unless diversity)***:
28 U.S.C. 1332(d)(2)

Brief description of cause:
Class Action Data Breach

VII. REQUESTED IN COMPLAINT:

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

DEMAND $ 5,000,000.00

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

VIII. RELATED CASE(S) IF ANY

(See instructions): JUDGE _____ DOCKET NUMBER 3:23-cv-697; 3:23-cv-701

DATE 07/26/2023

SIGNATURE OF ATTORNEY OF RECORD /s/ Gary M. Klinger

FOR OFFICE USE ONLY

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

INSTRUCTIONS FOR ATTORNEYS COMPLETING CIVIL COVER SHEET FORM JS 44

Authority For Civil Cover Sheet

The JS 44 civil cover sheet and the information contained herein neither replaces nor supplements the filings and service of pleading or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. Consequently, a civil cover sheet is submitted to the Clerk of Court for each civil complaint filed. The attorney filing a case should complete the form as follows:

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

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

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

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

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

IV. **Nature of Suit.** Place an "X" in the appropriate box. If the nature of suit cannot be determined, be sure the cause of action, in Section VI below, is sufficient to enable the deputy clerk or the statistical clerk(s) in the Administrative Office to determine the nature of suit. If the cause fits more than one nature of suit, select the most definitive.

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. When the petition for removal is granted, check this box.
Remanded from Appellate Court. (3) Check this box for cases remanded to the district court for further action. Use the date of remand as the filing date.
Reinstated or Reopened. (4) Check this box for cases reinstated or reopened in the district court. Use the reopening date as the filing date.
Transferred from Another District. (5) For cases transferred under Title 28 U.S.C. Section 1404(a). Do not use this for within district transfers or multidistrict litigation transfers.
Multidistrict Litigation – Transfer. (6) Check this box when a multidistrict case is transferred into the district under authority of Title 28 U.S.C. Section 1407.
Multidistrict Litigation – Direct File. (8) Check this box when a multidistrict case is filed in the same district as the Master MDL docket.
PLEASE NOTE THAT THERE IS NOT AN ORIGIN CODE 7. Origin Code 7 was used for historical records and is no longer relevant due to changes in 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.

AO 440 (Rev. 06/12) Summons in a Civil Action

UNITED STATES DISTRICT COURT

for the

Northern District of Indiana

MARK KUHN, on behalf of himself and all others similarly situated,

Plaintiff(s)

v.

1ST SOURCE BANK,

Defendant(s)

Civil Action No.

SUMMONS IN A CIVIL ACTION

To: *(Defendant's name and address)* 1st Source Bank
c/o Registered Agent
100 North Michigan Street
South Bend, Indiana 46601

A lawsuit has been filed against you.

Within 21 days after service of this summons on you (not counting the day you received it) — or 60 days if you are the United States or a United States agency, or an officer or employee of the United States described in Fed. R. Civ. P. 12 (a)(2) or (3) — you must serve on the plaintiff an answer to the attached complaint or a motion under Rule 12 of the Federal Rules of Civil Procedure. The answer or motion must be served on the plaintiff or plaintiff's attorney, whose name and address are: Gary M. Klinger
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606

If you fail to respond, judgment by default will be entered against you for the relief demanded in the complaint. You also must file your answer or motion with the court.

CLERK OF COURT

Date: _____

_____
Signature of Clerk or Deputy Clerk

Civil Action No.

PROOF OF SERVICE

(This section should not be filed with the court unless required by Fed. R. Civ. P. 4 (l))

This summons for *(name of individual and title, if any)* _____ was received by me on *(date)* _____ .

❒ I personally served the summons on the individual at *(place)* _____ on *(date)* _____ ; or

❒ I left the summons at the individual's residence or usual place of abode with *(name)* _____ , a person of suitable age and discretion who resides there, on *(date)* _____ , and mailed a copy to the individual's last known address; or

❒ I served the summons on *(name of individual)* _____ , who is designated by law to accept service of process on behalf of *(name of organization)* _____ on *(date)* _____ ; or

❒ I returned the summons unexecuted because _____ ; or

❒ Other *(specify):*

My fees are $ _____ for travel and $ _____ for services, for a total of $ 0.00 .

I declare under penalty of perjury that this information is true.

Date: _____

_____
Server's signature

_____
Printed name and title

_____
Server's address

Additional information regarding attempted service, etc: