UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF INDIANA
SOUTH BEND DIVISION

PAMELA TOMPACH on behalf of herself and all others similarly situated, Plaintiff, v. **1st SOURCE CORPORATION and 1st SOURCE BANK,** Defendants.	Case No. 3:23-cv-23-711 **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Pamela Tompach ("Plaintiff"), by and through her undersigned counsel, individually and on behalf of all similarly situated persons, alleges the following against 1st Source Corporation, 1st Source Bank, and any affiliates (collectively, "1st Source" or "Defendant") based upon personal knowledge with respect to herself and on information and belief derived from, among other things, investigation by her counsel and review of public documents as to all other matters:

I. INTRODUCTION

1. Plaintiff brings this class action against 1st Source for its failure to properly secure and safeguard her and roughly 450,000 similarly situated individuals' names, Social Security numbers, driver's license or state identification card numbers, other government-issued identification numbers, and dates of birth (the "Private Information") from hackers.

2. 1st Source, based in South Bend, Indiana, is a locally controlled financial institution headquartered in the northern Indiana-southwestern Michigan area.

3. On or about July 19, 2023, 1st Source filed a data breach notification with the Attorney General of Maine. Around the same time, 1st Source also sent out data breach letters (the "Notice") to individuals whose Private Information was compromised as a result of the hacking incident.

4. Based on the Notice, 1st Source became aware of a critical vulnerability impacting its secure file transfer solution and conducted an investigation that determined that third parties gained access to and "may have" acquired its customers' files, including Plaintiff's and Class Members' Private Information (the "Data Breach").

5. In response, 1st Source is providing affected customers with access to up to twelve (12) months of credit monitoring and identity protection services.

6. Plaintiff and "Class Members" (defined below) were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm. The risk will remain for their respective lifetimes.

7. The Private Information compromised in the Data Breach included highly sensitive data that represents a gold mine for data thieves, including but not limited to, names and Social Security numbers that 1st Source collected and failed to protect. Now armed with the Private Information accessed in the Data Breach, data thieves can commit a variety of crimes including, *e.g.*, opening new financial accounts in Class Members' names, taking out loans in Class Members' names, obtaining government benefits, filing fraudulent tax returns, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

8. There has been no assurance offered by 1st Source that all personal data or copies of data have been recovered or destroyed, or that Defendant has adequately enhanced its data

security supervisory and monitoring practices sufficient to avoid a similar breach of its customers' Private Information in the future.

9. Therefore, Plaintiff and Class Members have suffered and are at an imminent, immediate, and continuing increased risk of suffering ascertainable losses in the form of harm from identity theft and other fraudulent misuse of their Private Information, the loss of the benefit of their bargain, out-of-pocket expenses incurred to remedy or mitigate the effects of the Data Breach, and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach.

10. Plaintiff brings this class action lawsuit to address 1st Source's inadequate safeguarding and supervision of Class Members' Private Information that it collected.

11. The potential for improper disclosure and theft of Plaintiff's and Class Members' Private Information was a known risk to 1st Source, and thus 1st Source was on notice that failing to take necessary steps to secure the Private Information left such Information vulnerable to unauthorized acquisition.

12. 1st Source failed to properly monitor the computer network and systems that housed the Private Information. Had 1st Source properly monitored and provided adequate supervision over its agents, vendors, and/or suppliers, it would have discovered the system vulnerability at issue sooner and prevented the Data Breach.

13. 1st Source also could have prevented the compromise of its clients' Private Information had it limited the types of information it shared with its vendors and employed reasonable supervisory measures to ensure that adequate data security practices, procedures, and protocols were being implemented and maintained by said vendors in order to secure and protect its customers' data.

14. Plaintiff's and Class Members' identities are now at risk because of 1st Source's negligent conduct as the Private Information that 1st Source collected and maintained is now in the hands of data thieves and other unauthorized third parties.

15. Plaintiff seeks to remedy these harms on behalf of herself and all similarly situated individuals whose Private Information was accessed and/or compromised during the Data Breach.

16. Accordingly, Plaintiff, on behalf of herself and the Class, asserts claims for negligence, breach of contract, breach of implied contract, invasion of privacy, unjust enrichment, and declaratory/injunctive relief.

II. PARTIES

17. Plaintiff Pamela Tompach is, and at all times mentioned herein was, a citizen of the State of Indiana.

18. Defendant 1st Source is headquartered in the northern Indiana-southwestern Michigan area, with locations in South Bend, Indiana in St. Joseph County.

III. JURISDICTION AND VENUE

19. The Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. Upon information and belief, the number of class members is over 100, many of whom have different citizenship from 1st Source. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

20. This Court has jurisdiction over 1st Source because 1st Source operates in and/or is incorporated in this District.

21. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events giving rise to this action occurred in this District and 1st Source has harmed Class Members residing in this District.

IV. FACTUAL ALLEGATIONS

A. 1st Source's Business and Collection of Plaintiff's and Class Members' Private Information

22. 1st Source is the largest locally controlled financial institution in the northern Indiana-southwestern Michigan area with nearly $8 billion in assets and more than 1,100 employees.[1]

23. As a condition of receiving banking and other financial services from 1st Source, Plaintiff was required to entrust it with her highly sensitive personal information.

24. In its "1st Source Bank Privacy Notice" (the "Privacy Policy"), 1st Source promises its customers that it will not share their Private Information with third parties without their consent. The Privacy Policy also highlights the different reasons 1st Source shares its customers' Private Information, including "[f]or our marketing purposes" and "joint marketing with other financial companies."[2] and that it is "committed to protecting our members' privacy."[3]

25. Thus, 1st Source promises its customers that it will keep their Private Information private; comply with industry standards related to data security and the maintenance of their Private Information; inform them of its legal duties relating to data security and comply with all federal and state laws protecting their Private Information; only use and release their Private

[1] *See* https://www.1stsource.com/about/ (last visited on July 26, 2023).
[2] *See* https://www.1stsource.com/app/uploads/2023/05/1stSource_PrivacyNotice_5-23_Fillable.pdf?x29779 (last visited on July 26, 2023).
[3] Privacy & Security Policy, https://1st Sourcecreditunion.org/privacy-security-policy/ (last visited on July 10, 2023).

Information for reasons that relate to the services it provides; and provide adequate notice to them if their Private Information is disclosed without authorization.

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

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

B. The Data Breach

28. Upon information and belief, a vulnerability in 1st Source's vendor's internal file transfer system was first discovered in late May of 2023.

29. 1st Source failed to adequately monitor its vendor's systems and timely detect the Breach.

30. Through the Data Breach, which was carried out by the notorious Clop ransomware gang, the unauthorized cybercriminals were able to access a cache of highly sensitive Private Information, including Plaintiff's and Class Members' names, Social Security numbers, and other government-issued identification numbers.

31. Upon information and belief, Clop knew of 1st Source's vendor's system vulnerability and had been exploiting it before it was discovered by 1st Source or the agents, contractors, vendors, and/or suppliers 1st Source supervised (or failed to adequately supervise).

32. 1st Source had obligations created by contract, industry standards, common law, and representations made to Plaintiff and Class Members to keep Plaintiff's and Class Members' Private Information confidential and to protect it from unauthorized access and disclosure.

33. Plaintiff and Class Members provided their Private Information to 1st Source with the reasonable expectation and mutual understanding that 1st Source would comply with its obligations to keep such information confidential and secure from unauthorized access and to provide timely notice of any security breaches.

34. 1st Source's data security obligations were particularly important given the substantial increase in cyberattacks on financial institutions in recent years.

35. 1st Source knew or should have known that its members' records would be targeted by cybercriminals. However, it failed to adequately monitor its agents, contractors, vendors, and/or suppliers in the handling and securing of Plaintiff's and Class Members' Private Information and thus failed to maintain reasonable security safeguards and protocols to protect the Class's Private Information, rendering them easy targets for cybercriminals.

C. 1st Source Failed to Comply with FTC Guidelines

36. 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. Indeed, the FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

37. In October 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cybersecurity guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they collect, 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. 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 into 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.

38. The FTC further recommends that companies not maintain personally identifiable information ("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 the network for suspicious activity, *and verify that third-party service providers have implemented reasonable security measures*.

39. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data by 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 the FTCA. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

40. As evidenced by the Data Breach, 1st Source failed to properly verify that its third-party service providers had implemented reasonable and basic security measures. 1st Source's failure in this regard constitutes an unfair act or practice prohibited by Section 5 of the FTCA.

41. 1st Source was at all times fully aware of its obligation to protect the Private Information of its customers yet failed to comply with such obligations. Defendant was also aware of the significant repercussions that would result from its failure to do so.

D. 1st Source Failed to Comply with Industry Standards

42. As noted above, experts studying cybersecurity routinely identify businesses as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

43. Some general industry best practices that Defendant should have required its vendor to implement include but are not limited to educating all employees, using only strong password requirements, implementing multilayer security including firewalls, anti-virus and anti-malware software, using encryption, requiring multi-factor authentication, backing up data, and limiting which employees can access sensitive data. As evidenced by the Data Breach, Defendant failed to ensure that its vendor was following some or all of these industry best practices.

44. Defendant failed to ensure that its vendor was in compliance with these accepted standards, thereby permitting the Data Breach to occur.

E. 1st Source Failed to Comply with the Law Concerning the Protection of Financial Institution Customers' Personal Information

45. Section 501(b) of the Gramm-Leach-Bliley Act states in relevant part that bank regulators must establish regulations, which banks must comply with, that "insure the security and confidentiality of customer records and information," "protect against any anticipated threats or hazards to the security or integrity of such records," and "protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer."[4] The regulation's provisions became effective in July 2001 and have steered the discussion of customer information protection in banking ever since. Nevertheless, as the Data Breach demonstrates, Defendant failed to live up to these cybersecurity obligations.

46. The Federal Deposit Insurance Corporation ("FDIC") guidance to banks regarding unauthorized access to customer information defines "sensitive customer information" to mean "a customer's name, address or telephone number in conjunction with the customer's Social Security

[4] *See also* FDIC Financial Institution Letter FIL-68-2001 *available at* https://www.fdic.gov/news/inactive-financial-institution-letters/2001/fil0168a.html (last visited May 1, 2023).

number, driver's license number, account number, credit or debit card number, or a personal identification number or password that would permit access to the customer's account."[5]

47. Here, Defendant's Notice confirms that the Data Breach concerned its customers' names, Social Security numbers, and other account information. As such, there is no question that the data involved here is what the FDIC would term sensitive customer information.

48. FDIC guidance further requires banks to notify its customers of a data breach "whenever it becomes aware of an incident of unauthorized access to customer information and, at the conclusion of a reasonable investigation, determines that misuse of the information has occurred or it is reasonably possible that misuse will occur."[6] In interpreting this guidance, banking industry groups recommend that banks provide notice to their customers "as soon as possible."[7]

49. In addition, federal regulations require banks to closely oversee security of third-party vendors. Given the circumstances of the instant Data Breach, it is apparent that Defendant also failed to fulfill this requirement.

F. 1st Source Breached its Duty to Safeguard Plaintiff's and Class Members' Private Information

50. In addition to its obligations under federal laws and regulations, 1st Source owed a duty to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information from being compromised, lost, stolen, accessed, and misused by unauthorized persons. 1st Source owed a duty to Plaintiff and Class Members to provide reasonable security, including complying with industry standards and

[5] FIL-27-2005 (April 1., 2005) *available at* https://www.fdic.gov/news/financial-institution-letters/2005/fil2705.html (last visited May 1, 2023).
[6] *Id.*
[7] American Bankers Association, Data Security & Customer Notification Requirements for Banks, *available at* https://www.aba.com/banking-topics/technology/data-security/data-security-customer-notification.

requirements, adequate monitoring of its employees, agents, and vendors, and ensuring that its vendor's computer systems, networks, and protocols adequately protected the Private Information of Class Members.

51. 1st Source breached its obligations to Plaintiff and Class Members and/or was otherwise negligent and reckless because it failed to properly monitor, maintain and safeguard its Plaintiff's and Class Members' Private Information. 1st Source's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to adequately protect its customers' Private Information;

b. Failing to sufficiently monitor its employees, agents, and vendors regarding the proper handling of its customers' Private Information;

c. Failing to fully comply with FTC guidelines for cybersecurity in violation of the FTCA;

d. Failing to adhere to industry standards for cybersecurity as discussed above; and

e. Otherwise breaching its duties and obligations to protect Plaintiff's and Class Members' Private Information.

52. Had 1st Source properly monitored and supervised its vendor's data security policies and procedures, it could have remedied the deficiencies in its vendor's information storage and security systems and required that it adopt security measures recommended by experts in the field. These simple acts could have helped to prevent intrusion into its vendor's information storage and security systems and, ultimately, the theft of Plaintiff's and Class Members' confidential Private Information.

53. Accordingly, Plaintiff's and Class Members' lives were severely disrupted by the Data Breach. What's more, they have been harmed as a result of the Data Breach and now face an

increased risk of future harm that includes, but is not limited to, fraud and identity theft. Plaintiff and Class Members also lost the benefit of the bargain they made with 1st Source.

G. 1st Source Should Have Known that Cybercriminals Target Private Information to Carry Out Fraud and Identity Theft

54. The FTC hosted a workshop to discuss "informational injuries," which are injuries that consumers like Plaintiff and Class Members suffer from privacy and security incidents such as data breaches or unauthorized disclosure of data.[8] Exposure of highly sensitive personal information that a consumer wishes to keep private may cause harm to the consumer, such as the ability to obtain or keep employment. Consumers' loss of trust in e-commerce also deprives them of the benefits provided by the full range of goods and services available which can have negative impacts on daily life.

55. Any victim of a data breach is exposed to serious ramifications regardless of the nature of the data that was breached. Indeed, the reason why cybercriminals like the Clop ransomware gang steal information is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims or to take over victims' identities in order to engage in illegal financial transactions under the victims' names.

56. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity or to otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more

[8] *FTC Information Injury Workshop, BE and BCP Staff Perspective,* Federal Trade Commission, (October 2018), *available at* https://www.ftc.gov/system/files/documents/reports/ftc-informational-injury-workshop-be-bcp-staff-perspective/informational_injury_workshop_staff_report_-_oct_2018_0.pdf (last visited on April 29, 2023).

information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

57. In fact, as technology advances, computer programs may scan the Internet with a wider scope to create a mosaic of information that may be used to link compromised information to an individual in ways that were not previously possible. This is known as the "mosaic effect." Names and dates of birth, combined with contact information like telephone numbers and email addresses, are very valuable to hackers and identity thieves as it allows them to access users' other accounts.

58. Thus, even if certain information was not purportedly involved in the Data Breach, the unauthorized parties could use Plaintiff's and Class Members' Private Information to access accounts, including, but not limited to, email accounts and financial accounts, to engage in a wide variety of fraudulent activity against Plaintiff and Class Members.

59. For these reasons, the FTC recommends that identity theft victims take several time-consuming steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert on their account (and an extended fraud alert that lasts for 7 years if someone steals the victim's identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a freeze on their credit, and correcting their credit reports.[9] However, these steps do not guarantee protection from identity theft but can only mitigate identity theft's long-lasting negative impacts.

[9] *See IdentityTheft.gov*, Federal Trade Commission, *available at* https://www.identitytheft.gov/Steps (last visited April 29, 2023).

60. Identity thieves can also use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, bank fraud, to obtain a driver's license or official identification card in the victim's name but with the thief's picture, to obtain government benefits, or to file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house in the victim's name, and even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

61. PII is data that can be used to detect a specific individual. PII is a valuable property right. Its value is axiomatic, considering the value of big data in corporate America and the consequences of cyber thefts (which include heavy prison sentences). Even this obvious risk-to-reward analysis illustrates beyond doubt that PII has considerable market value.

62. The U.S. Attorney General stated in 2020 that consumers' sensitive personal information commonly stolen in data breaches "has economic value."[10] The increase in cyberattacks, and attendant risk of future attacks, was widely known and completely foreseeable to the public and to anyone in Defendant's industry, including Defendant.

63. The PII of consumers 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, PII can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[11] Experian reports that a stolen credit or debit card number can

[10] *See Attorney General William P. Barr Announces Indictment of Four Members of China's Military for Hacking into Equifax*, U.S. Dep't of Justice, Feb. 10, 2020, available at https://www.justice.gov/opa/speech/attorney-general-william-p-barr-announces-indictment-fourmembers-china-s-military (last visited on April 29, 2023).

[11] *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 on April 29, 2023).

sell for $5 to $110 on the dark web and that the "*fullz*" (a term criminals who steal credit card information use to refer to a complete set of information on a fraud victim) sold for $30 in 2017.[12]

64. Likewise, the value of PII is increasingly evident in our digital economy. Many companies including 1st Source collect PII for purposes of data analytics and marketing, as acknowledged in its Privacy Policy. These companies collect it to better target customers and share it with third parties for similar purposes.[13]

65. One author has noted: "Due, in part, to the use of PII in marketing decisions, commentators are conceptualizing PII as a commodity. Individual data points have concrete value, which can be traded on what is becoming a burgeoning market for PII."[14]

66. Consumers also recognize the value of their personal information and offer it in exchange for goods and services. The value of PII can be derived not only by a price at which consumers or hackers actually seek to sell it, but rather by the economic benefit consumers derive from being able to use it and control the use of it.

67. A consumer's ability to use their PII is encumbered when their identity or credit profile is infected by misuse or fraud. For example, a consumer with false or conflicting information on their credit report may be denied credit. Also, a consumer may be unable to open an electronic account where their email address is already associated with another user. In this sense, among others, the theft of PII in the Data Breach led to a diminution in value of the PII.

---

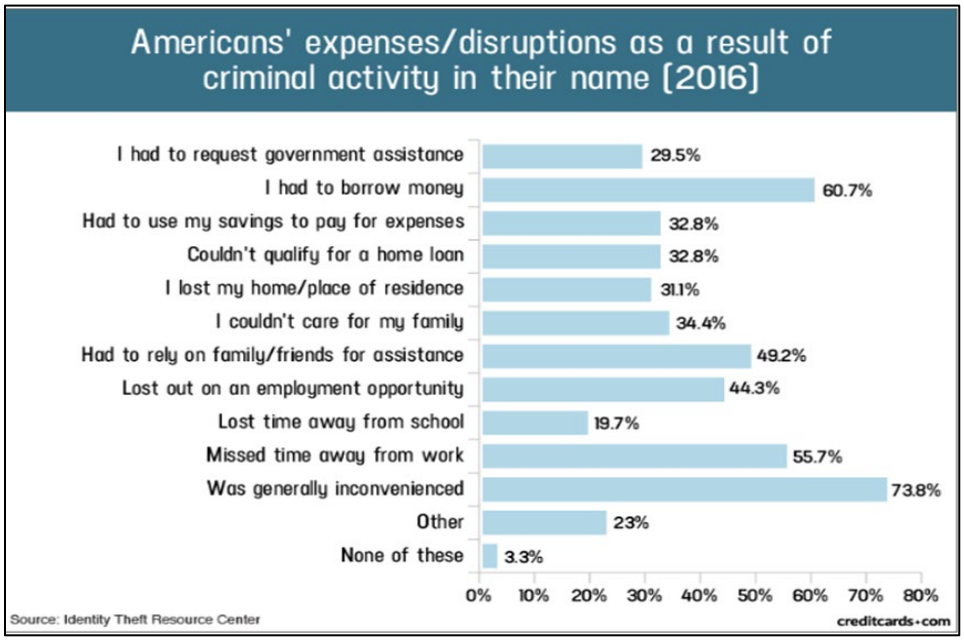
[12] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited on April 29, 2023).

[13] *See* https://robinhood.com/us/en/support/articles/privacy-policy/ (last visited on April 29, 2023).

[14] *See* John T. Soma, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ('PII') Equals the "Value" of Financial Assets,* 15 Rich. J. L. & Tech. 11, 14 (2009).

68. Data breaches, like that at issue here, damage consumers by interfering with their fiscal autonomy. Any past and potential future misuse of Plaintiff's PII impairs their ability to participate in the economic marketplace.

69. A study by the Identity Theft Resource Center[15] shows the multitude of harms caused by fraudulent use of PII:



70. It must also be noted that there may be a substantial time lag between when harm occurs and when it is discovered, and also between when PII and/or personal financial information is stolen and when it is used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:[16]

> [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 have been sold or posted on

[15] Steele, Jason, *Credit Card and ID Theft Statistics*, CreditCards.com (October 23, 2017), *available at* https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276/ (last visited April 29, 2023).

[16] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO (June 2007), *available at* https://www.gao.gov/assets/270/262904.html (last visited April 29, 2023).

> 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.

71. PII is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black market" for years.

72. As a result, Plaintiff and Class Members are at an increased risk of fraud and identity theft for many years into the future. Thus, Plaintiff and Class Members have no choice but to vigilantly monitor their accounts for many years.

H. Plaintiff's and Class Members' Damages

73. Plaintiff and Class Members have been damaged by the compromise of their Private Information in the Data Breach.

74. In order to receive banking and other financial services from Defendant, she had to disclose her Private Information to Defendant.

75. Since the Data Breach, Plaintiff has been forced to spend more time than ever before monitoring her accounts for fraudulent activity.

76. Plaintiff and Class Members entrusted their Private Information to Defendant in order to receive Defendant's services.

77. Their Private Information was subsequently compromised as a direct and proximate result of the Data Breach, which Data Breach resulted from Defendant's inadequate data security monitoring and supervisory practices.

78. As a direct and proximate result of 1st Source's actions and omissions, Plaintiff and Class Members have been harmed and are at an imminent, immediate, and continuing increased risk of harm, including but not limited to, having loans opened in their names, tax returns filed in

their names, utility bills opened in their names, credit card accounts opened in their names, and other forms of identity theft.

79. Further, as a direct and proximate result of 1st Source's conduct, Plaintiff and Class Members have been forced to spend time dealing with the effects of the Data Breach.

80. Plaintiff and Class Members also face a substantial risk of being targeted in future phishing, data intrusion, and other illegal schemes through the misuse of their Private Information, since potential fraudsters will likely use such Private Information to carry out such targeted schemes against Plaintiff and Class Members.

81. The Private Information maintained by and stolen from Defendant's systems, combined with publicly available information, allows nefarious actors to assemble a detailed mosaic of Plaintiff and Class Members, which can also be used to carry out targeted fraudulent schemes against Plaintiff and Class Members.

82. Plaintiff suffered actual injury from the exposure of her Private Information, which violates her right to privacy.

83. Plaintiff has and will continue to spend considerable time and effort monitoring her accounts to protect herself from identity theft. Plaintiff fears for her personal financial security and uncertainty over what other PII may have been exposed in the Data Breach. Plaintiff has and is experiencing feelings of anxiety, stress, fear, and frustration because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

84. Plaintiff and Class Members also suffered actual injury in the form of damages to and diminution in the value of her PII. After all, PII is a form of intangible property – property that Defendant was required to adequately protect.

85. Moreover, Plaintiff and Class Members have an interest in ensuring that their Private Information, which is believed to still be in the possession of 1st Source and its vendors, suppliers, and/or agents, is protected from future additional breaches by the implementation of more adequate data security measures and safeguards, including but not limited to, ensuring that the storage of data or documents containing personal and financial information is not accessible online, that access to such data is password-protected, and that such data is properly encrypted.

86. As a direct and proximate result of 1st Source's actions and inactions, Plaintiff and Class Members have suffered a loss of privacy and have suffered cognizable harm, including an imminent and substantial future risk of harm, in the forms set forth above.

V. CLASS ACTION ALLEGATIONS

87. Plaintiff brings this action individually and on behalf of all other persons similarly situated, pursuant to Federal Rule of Civil Procedure 23(a), 23(b)(1), 23(b)(2), and 23(b)(3).

88. Specifically, Plaintiff proposes the following Nationwide Class (also referred to herein as the "Class"), subject to amendment as appropriate:

> **Nationwide Class**
>
> All individuals in the United States who had Private Information accessed and/or acquired as a result of the Data Breach, including all who were sent a notice of the Data Breach.

89. Excluded from the Class are Defendant and its parents or subsidiaries, any entities in which it has a controlling interest, as well as its officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns. Also excluded is any Judge to whom this case is assigned as well as their judicial staff and immediate family members.

90. Plaintiff reserves the right to modify or amend the definitions of the proposed Class, as well as add subclasses, before the Court determines whether certification is appropriate.

91. The proposed Class meets the criteria for certification under Fed. R. Civ. P. 23(a), (b)(2), and (b)(3).

92. Numerosity. The Class Members are so numerous that joinder of all members is impracticable. Though the exact number and identities of Class Members are unknown at this time, based on information and belief, the Class consists of roughly 450,000 customers of 1st Source whose data was compromised in the Data Breach. The identities of Class Members are ascertainable through 1st Source's records, Class Members' records, publication notice, self-identification, and other means.

93. Commonality. There are questions of law and fact common to the Class which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether 1st Source engaged in the conduct alleged herein;

b. When 1st Source actually learned of its vendor's system vulnerability and resulting Data Breach;

c. Whether 1st Source's response to the Data Breach was adequate;

d. Whether 1st Source unlawfully lost or disclosed Plaintiff's and Class Members' Private Information;

e. Whether 1st Source failed to implement and maintain reasonable monitoring and supervisory procedures and practices appropriate to the nature and scope of the Private Information compromised in the Data Breach;

f. Whether 1st Source adequately ensured that its vendor's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

g. Whether 1st Source owed a duty to Class Members to safeguard their Private Information;

h. Whether 1st Source breached its duty to Class Members to safeguard their Private Information;

i. Whether hackers acquired and obtained Class Members' Private Information via the Data Breach;

j. Whether 1st Source knew or should have known that its vendor's data security systems and monitoring processes were deficient;

k. What damages Plaintiff and Class Members suffered as a result of 1st Source's misconduct;

l. Whether 1st Source's conduct was negligent;

m. Whether 1st Source was unjustly enriched;

n. Whether Plaintiff and Class Members are entitled to actual and/or statutory damages;

o. Whether Plaintiff and Class Members are entitled to additional credit and identity monitoring and monetary relief; and

p. Whether Plaintiff and Class Members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

94. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's Private Information, like that of every other Class Member, was compromised in the Data Breach.

95. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of Class Members. Plaintiff's counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

96. Predominance. 1st Source has engaged in a common course of conduct toward Plaintiff and Class Members in that all of Plaintiff's and Class Members' data was stored on the same computer systems and unlawfully accessed and exfiltrated in the same way. The common issues arising from 1st Source's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

97. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of this controversy and no unusual difficulties are likely to be encountered in the management of this class action. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a Class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for 1st Source. In contrast, conducting this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

98. Class certification is also appropriate under Fed. R. Civ. P. 23(b)(2). 1st Source has acted and/or refused to act on grounds generally applicable to the Class such that final injunctive relief and/or corresponding declaratory relief is appropriate as to the Class as a whole.

99. Finally, all members of the proposed Class are readily ascertainable. 1st Source has access to the names and addresses and/or email addresses of Class Members affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by 1st Source.

VI. CLAIMS FOR RELIEF

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

100. Plaintiff restates and realleges all of the allegations stated in the preceding paragraphs as if fully set forth herein.

101. 1st Source knowingly collected Plaintiff's and Class Members' Private Information and had a duty to exercise reasonable care in safeguarding, securing, and protecting such Information from being disclosed, compromised, lost, stolen, and misused by unauthorized parties.

102. 1st Source knew or should have known of the risks inherent in collecting the Private Information of Plaintiff and Class Members and the importance of adequate data security. 1st Source was on notice because, on information and belief, it knew or should have known that it would be an attractive target for cyberattacks.

103. 1st Source owed a duty of care to Plaintiff and Class Members whose Private Information was entrusted to it. 1st Source's duties included, but were not limited to, the following:

a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, monitoring, deleting, and protecting the Private Information;

b. To protect its customers' Private Information using (and/or ensuring that its vendors, suppliers, and/or agents used) reasonable and adequate security procedures, practices, and protocols compliant with industry standards;

c. To have employee, agent, and vendor monitoring procedures in place to prevent the loss or unauthorized dissemination of Private Information in its possession; and

d. To employ reasonable data security measures and otherwise protect the Private Information of Plaintiff and Class Members pursuant to the FTCA.

104. 1st Source's duty to employ reasonable data security measures arose, in part, 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.

105. 1st Source's duty also arose because Defendant was bound by industry standards to protect its customers' confidential Private Information.

106. Plaintiff and Class Members were foreseeable victims of any inadequate security practices on the part of Defendant, and 1st Source owed them a duty of care to not subject them to an unreasonable risk of harm.

107. 1st Source breached its duties by failing to exercise reasonable care in supervising its agents, contractors, vendors, and suppliers, and in handling and securing the Private Information of Plaintiff and Class Members, which failures actually and proximately caused the Data Breach and Plaintiff's and Class Members' injuries. As a direct and traceable result of Defendant's negligence and/or negligent supervision, Plaintiff and Class Members have suffered or will suffer

damages, including monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

108. 1st Source had a special relationship with Plaintiff and Class Members. Plaintiff's and Class Members' willingness to entrust 1st Source with their Private Information was predicated on the understanding that 1st Source would take adequate security precautions to protect it.

109. 1st Source's breach of duties owed to Plaintiff and Class Members caused Plaintiff's and Class Members' Private Information to be compromised, exfiltrated, and misused, as alleged herein.

110. 1st Source's breaches of duties owed to Plaintiff and Class Members also caused a substantial, imminent risk to Plaintiff and Class Members of identity theft, loss of control over their Private Information, and/or loss of time and money to monitor their accounts for fraud.

111. As a result of 1st Source's negligence in breach of its duties owed to Plaintiff and Class Members, Plaintiff and Class Members are in danger of imminent harm in that their Private Information, which is still in the possession of third parties, will be used for fraudulent purposes.

112. 1st Source also had independent duties under federal and state law that required it to reasonably safeguard Plaintiff's and Class Members' Private Information and promptly notify them about the Data Breach.

113. As a direct and proximate result of 1st Source's negligent conduct, Plaintiff and Class Members have suffered damages as alleged herein and are at imminent risk of further harm.

114. The injury and harm that Plaintiff and Class Members suffered was reasonably foreseeable.

115. Plaintiff and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

116. In addition to monetary relief, Plaintiff and Class Members are also entitled to injunctive relief requiring 1st Source to, *inter alia*, strengthen its data security systems and supervision procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiff and Class Members.

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

117. Plaintiff restates and realleges the allegations in the preceding paragraphs as if fully set forth herein.

118. Plaintiff and Class Members entered into a valid and enforceable contract through which they turned over their valuable Private Information to 1st Source in exchange for banking services. That contract included promises by Defendant to secure, safeguard, and not disclose Plaintiff's and Class Members' Private Information to unauthorized third parties.

119. 1st Source's Privacy Policy memorialized the rights and obligations of 1st Source and its customers. This document was provided to Plaintiff and Class Members in a manner in which it became part of the agreement for services.

120. In the Privacy Policy, 1st Source commits to protecting the privacy and security of its members highly sensitive private information and promises to never share Plaintiff's and Class Members' Private Information except under certain limited circumstances.

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

122. However, 1st Source did not secure, safeguard, and/or keep private Plaintiff's and Class Members' Private Information, and therefore 1st Source breached its contracts with Plaintiff and Class Members.

123. 1st Source allowed third parties to access, copy, and exfiltrate Plaintiff's and Class Members' Private Information without permission. Therefore, 1st Source breached the Privacy Policy with Plaintiff and Class Members.

124. 1st Source's failure to satisfy its confidentiality and privacy obligations resulted in 1st Source providing services to Plaintiff and Class Members that were of a diminished value.

125. As a result, Plaintiff and Class Members have been harmed, damaged, and/or injured as described herein, including in Defendant's failure to fully perform its part of the bargain with Plaintiff and Class Members.

126. As a direct and proximate result of 1st Source's conduct, Plaintiff and Class Members suffered and will continue to suffer damages in an amount to be proven at trial.

127. In addition to monetary relief, Plaintiff and Class Members are also entitled to injunctive relief requiring 1st Source to, *inter alia*, strengthen its data security systems and supervision procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiff and Class Members.

COUNT III
BREACH OF IMPLIED CONTRACT
(On behalf of Plaintiff and the Class)

128. Plaintiff restates and realleges the allegations in the preceding paragraphs as if fully set forth herein.

129. This Count is pleaded in the alternative to Count II above.

130. 1st Source provides banking services to Plaintiff and Class Members. Plaintiff and Class Members formed an implied contract with Defendant regarding the provision of those

services through their collective conduct, including by Plaintiff and Class Members providing their valuable Private Information to Defendant in exchange for services from Defendant.

131. Through Defendant's provision of services to Plaintiff and Class Members, it knew or should have known that it was obligated to protect Plaintiff's and Class Members' confidential Private Information that they entrusted to it, and to do so in accordance with its policies, practices, and applicable law.

132. As consideration, Plaintiff and Class Members turned over valuable Private Information to 1st Source. Accordingly, Plaintiff and Class Members bargained with 1st Source to securely maintain and store their Private Information.

133. 1st Source accepted possession of Plaintiff's and Class Members' Private Information for the purpose of providing services to Plaintiff and Class Members.

134. In delivering their Private Information to 1st Source, Plaintiff and Class Members intended and understood that 1st Source would adequately safeguard it as part of that service.

135. Defendant's implied promises to Plaintiff and Class Members include, but are not limited to, (1) taking steps to ensure that anyone who is granted access to Private Information also protect the confidentiality of that data; (2) taking steps to ensure that the Private Information that is placed in the control of its employees, agents, vendors, and/or suppliers is restricted and limited to achieve an authorized business purpose; (3) restricting access to qualified and trained employees, agents, vendors, and/or suppliers; (4) designing and implementing appropriate supervision policies, practices, and procedures to protect the Private Information against criminal data breaches; (5) applying or requiring proper encryption of the Private Information; (6) implementing or requiring the implementation of multifactor authentication for access; and (7) taking other steps to protect against foreseeable data breaches.

136. Plaintiff and Class Members would not have entrusted their Private Information to 1st Source in the absence of such an implied contract.

137. Had 1st Source disclosed to Plaintiff and the Class that they did not have adequate security monitoring or supervisory practices to ensure its vendor would secure their sensitive data, Plaintiff and Class Members would not have banked with 1st Source and thus would not have provided 1st Source with their Private Information.

138. 1st Source recognized that Plaintiff's and Class Member's Private Information was highly sensitive and must be protected, and that this protection was of material importance as part its bargain with Plaintiff and the other Class Members.

139. 1st Source violated these implied contracts by failing to employ reasonable and adequate security measures to ensure the security of Plaintiff's and Class Members' Private Information.

140. Plaintiff and Class Members have been damaged by 1st Source's conduct, including the harms and injuries arising from the Data Breach now and in the future, as alleged herein.

COUNT IV
INVASION OF PRIVACY
(On behalf of Plaintiff and the Class)

141. Plaintiff restates and realleges the allegations in the preceding paragraphs as if fully set forth herein.

142. Plaintiff and Class Members maintain a privacy interest in their Private Information, which is private, confidential information that is also protected from disclosure by contract and applicable laws and regulations set forth above.

143. Additionally, Plaintiff's and Class Members' Private Information is highly attractive to criminals who can nefariously use such Private Information to commit and profit from fraud, identity theft, and other crimes without the victims' knowledge and consent.

144. The unauthorized disclosure and acquisition of Plaintiff's and the Class's Private Information by a cybercriminal third party is highly offensive to a reasonable person. Defendant's reckless and negligent failure to protect Plaintiff's and the Class's Private Information constitutes an intentional interference with Plaintiff's and Class Members' interest in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

145. Defendant acted with a knowing state of mind when it permitted the Data Breach because it knew its vendor's information security practices were inadequate yet failed to adequately monitor and supervise its vendor and/or require that its vendor implement proper information security practices sufficient to safeguard Plaintiff's and Class Members' Private Information.

146. Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the Class since their Private Information is still maintained by Defendant and its vendors, suppliers, and/or agents with their inadequate cybersecurity system and policies still being observed.

147. Thus, Plaintiff seeks injunctive relief requiring 1st Source to, *inter alia*, strengthen its data security systems and supervisory procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiff and Class Members.

148. Plaintiff and Class Members also seek compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by Defendant, the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest, and costs.

COUNT V
UNJUST ENRICHMENT
(On behalf of Plaintiff and the Class)

149. Plaintiff restates and realleges the allegations in the preceding paragraphs as if fully set forth herein.

150. This Count is pleaded in the alternative to Counts II and III above.

151. Plaintiff and Class Members conferred a benefit on 1st Source by turning over their Private Information to Defendant in exchange for cybersecurity protection sufficient to protect their Private Information. Plaintiff and Class Members did not receive such protection.

152. Upon information and belief, 1st Source funds its data security measures entirely from its general revenue, which includes revenue from marketing Plaintiff's and Class Members' Private Information, as set forth in Defendant's Privacy Policy.

153. As such, a portion of such revenue is to be used to provide a reasonable and adequate level of data security that is in compliance with applicable state and federal regulations and industry standards, and the amount of the portion of its revenue that is allocated to data security is known to 1st Source.

154. 1st Source has retained the benefits of its unlawful conduct, including the amounts of revenue received from the use of Plaintiff's and Class Members' Private Information that should have been used for adequate cybersecurity practices that it did failed to provide.

155. 1st Source knew that Plaintiff and Class Members conferred a benefit upon it, which 1st Source accepted. 1st Source used the Private Information of Plaintiff and Class Members for business purposes and profited therefrom, while failing to use such revenue for adequate data security measures that would have secured Plaintiff's and Class Members' Private Information and prevented the Data Breach.

156. If Plaintiff and Class Members had known that 1st Source would not be able to ensure the security of their Private Information, they would not have agreed to provide their Private Information to Defendant in the first place.

157. Due to 1st Source's conduct alleged herein, it would be unjust and inequitable under the circumstances for 1st Source to be permitted to retain the benefit of its wrongful conduct.

158. As a direct and proximate result of 1st Source's conduct, Plaintiff and Class Members have suffered and/or are at a substantial and imminent risk of suffering injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity to control how their Private Information is used; (iii) the compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their Private Information, which remains 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 Private Information in its (and its vendor's) continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

159. Plaintiff and Class Members are entitled to full refunds, restitution, and/or damages from 1st Source and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by 1st Source from its wrongful conduct. This can be accomplished by

establishing a constructive trust from which the Plaintiff and Class Members may seek restitution or compensation.

160. Plaintiff and Class Members may not have an adequate remedy at law against 1st Source, and accordingly, they plead this claim for unjust enrichment in addition to, or in the alternative to, other claims pleaded herein.

COUNT VI
DECLARATORY JUDGMENT
(On behalf of Plaintiff and the Class)

161. Plaintiff restates and realleges the allegations in the preceding paragraphs as if fully set forth herein.

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

163. 1st Source owes a duty of care to Plaintiff and Class Members, which required it to adequately secure Plaintiff's and Class Members' Private Information.

164. 1st Source still possesses Private Information belonging to Plaintiff and Class Members.

165. Plaintiff alleges that 1st Source's data security measures remain inadequate. Furthermore, Plaintiff continues to suffer injury as a result of the compromise of her Private Information and the risk remains that further compromises of her Private Information will occur in the future.

166. Under its authority pursuant to the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. 1st Source owes a legal duty to secure its customers' Private Information and to timely notify customers of a data breach under the common law and Section 5 of the FTCA;

b. 1st Source's existing security measures do not comply with its explicit or implicit contractual obligations and duties of care to provide reasonable security procedures and practices that are appropriate to protect customers' Private Information; and

c. 1st Source continues to breach this legal duty by failing to employ reasonable measures to secure customers' Private Information.

167. This Court should also issue corresponding prospective injunctive relief requiring 1st Source to employ adequate security protocols consistent with legal and industry standards to protect customers' Private Information, including the following:

a. Order 1st Source to provide lifetime credit monitoring and identity theft insurance to Plaintiff and Class Members.

b. Order that, to comply with Defendant's explicit or implicit contractual obligations and duties of care, 1st Source must implement and maintain reasonable security measures, including, but not limited to:

i. engaging 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;

ii. engaging third-party security auditors and internal personnel to run automated security monitoring;

iii. auditing, testing, and training its security personnel regarding any new or modified procedures;

iv. segmenting its user applications by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of 1st Source's systems;

v. conducting regular database scanning and security checks;

vi. routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

vii. meaningfully educating its users about the threats they face with regard to the security of their Private Information, as well as the steps 1st Source's customers should take to protect themselves.

168. If an injunction is not issued, Plaintiff will suffer irreparable injury and will lack an adequate legal remedy to prevent another data breach at 1st Source. The risk of another such breach is real, immediate, and substantial. If another breach at 1st Source occurs, Plaintiff will not have an adequate remedy at law because many of the resulting injuries are not readily quantifiable.

169. The hardship to Plaintiff if an injunction does not issue exceeds the hardship to 1st Source if an injunction is issued. Plaintiff will likely be subjected to substantial, continued identity theft and other related damages if an injunction is not issued. On the other hand, the cost of 1st Source's compliance with an injunction requiring reasonable prospective data security measures is relatively minimal, and 1st Source has a pre-existing legal obligation to employ such measures.

170. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing a subsequent data breach at

1st Source, thus preventing future injury to Plaintiff and other customers whose Private Information would be further compromised.

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and the Class described above, seeks the following relief:

a. An order certifying this action as a Class action under Fed. R. Civ. P. 23, defining the Class as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiff is a proper representative of the Class requested herein;

b. Judgment in favor of Plaintiff and Class Members awarding them appropriate monetary relief, including actual damages, statutory damages, equitable relief, restitution, disgorgement, and statutory costs;

c. An order providing injunctive and other equitable relief as necessary to protect the interests of the Class as requested herein;

d. An order instructing 1st Source to purchase or provide funds for lifetime credit monitoring and identity theft insurance to Plaintiff and Class Members;

e. An order requiring 1st Source to pay the costs involved in notifying Class Members about the judgment and administering the claims process;

f. A judgment in favor of Plaintiff and Class Members awarding them prejudgment and post-judgment interest, reasonable attorneys' fees, costs, and expenses as allowable by law; and

g. An award of such other and further relief as this Court may deem just and proper.

DATED: July 26, 2023 Respectfully submitted,

/s/ Kathleen A. DeLaney
Kathleen A. DeLaney (#18604-49)
Christopher S. Stake (#27356-53)
DELANEY & DELANEY LLC
3646 North Washington Blvd.
Indianapolis, IN 46205
Telephone: (317) 920-0400
Email: kathleen@delaneylaw.net
cstake@delaneylaw.net

Mason A. Barney (*pro hac vice* forthcoming)
Tyler J. Bean (*pro hac vice* forthcoming)
SIRI & GLIMSTAD LLP
745 Fifth Avenue, Suite 500
New York, New York 10151
Telephone: (212) 532-1091
Email: mbarney@sirillp.com
Email: tbean@sirillp.com

DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury on all triable issues.

DATED: July 26, 2023

Respectfully submitted,

/s/ Kathleen A. DeLaney
Kathleen A. DeLaney (#18604-49)
Christopher S. Stake (#27356-53)
DELANEY & DELANEY LLC
3646 North Washington Blvd.
Indianapolis, IN 46205
Telephone: (317) 920-0400
Email: kathleen@delaneylaw.net
cstake@delaneylaw.net

Mason A. Barney (*pro hac vice* forthcoming)
Tyler J. Bean (*pro hac vice* forthcoming)
SIRI & GLIMSTAD LLP
745 Fifth Avenue, Suite 500
New York, New York 10151
Telephone: (212) 532-1091
Email: mbarney@sirillp.com
Email: tbean@sirillp.com

JS 44 (Rev. 10/20)

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

Pamela Tompach
on behalf of herself and all others similarly situated,

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

(c) Attorneys *(Firm Name, Address, and Telephone Number)*
Kathleen A. DeLaney, Esq. and Christopher S. Stake
DeLaney & DeLaney LLC, 3646 N. Washington Blvd.
Indianapolis, IN 46205; 317-920-0400

DEFENDANTS

1st SOURCE CORPORATION and 1st SOURCE BANK,

County of Residence of First Listed Defendant St. Joseph
(IN U.S. PLAINTIFF CASES ONLY)
NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

Attorneys *(If Known)*

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

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

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

(For Diversity Cases Only)

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

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

Click here for: Nature of Suit Code Descriptions.

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

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
- ☐ 835 Patent - Abbreviated New Drug Application
- ☐ 840 Trademark
- ☐ 880 Defend Trade Secrets Act of 2016

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

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

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

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:
Plaintiff brings this action against Defendant for their failure to properly secure and safeguard Plaintiff's private and personal information.

VII. REQUESTED IN COMPLAINT:

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

DEMAND $

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

VIII. RELATED CASE(S) IF ANY

(See instructions): JUDGE _____ DOCKET NUMBER _____

DATE
July 26, 2023

SIGNATURE OF ATTORNEY OF RECORD
/s/ Kathleen A. DeLaney

FOR OFFICE USE ONLY

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

INSTRUCTIONS FOR ATTORNEYS COMPLETING CIVIL COVER SHEET FORM JS 44

Authority For Civil Cover Sheet

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

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

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

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

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

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

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

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

Pamela Tompach on behalf of herself and all others similarly situated,

Plaintiff(s)

v.

1st Source Corporation and 1st Source Bank

Defendant(s)

Civil Action No.

SUMMONS IN A CIVIL ACTION

To: *(Defendant's name and address)*

1st Source Bank
c/o John B Griffith
1st Source Bank
100 N Michigan St.
South Bend, IN 46601 - 1000

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:

Kathleen A. Delaney, Esq.
DELANEY & DELANEY LLC
3646 North Washington Blvd.
Indianapolis, IN 46205
Tel: 317-920-0400
E: kathleen@delaneylaw.net

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:

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

UNITED STATES DISTRICT COURT

for the

Northern District of Indiana
South Bend Division

Pamela Tompach on behalf of herself and all others similarly situated,

Plaintiff(s)

v.

1st Source Corporation and 1st Source Bank

Defendant(s)

Civil Action No.

SUMMONS IN A CIVIL ACTION

To: *(Defendant's name and address)*

1st Source Corporation
c/o Andrea G Short
100 N Michigan Street,
South Bend, IN 46601-0000

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:

Kathleen A. Delaney, Esq.
DELANEY & DELANEY LLC
3646 North Washington Blvd.
Indianapolis, IN 46205
Tel: 317-920-0400
E: kathleen@delaneylaw.net

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: