

**IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA**

PATRICIA ANDROS and RONALD
SIMMONT, individually and on behalf of all
others similarly situated,

Plaintiffs,

v.

COMCAST CABLE COMMUNICATIONS,
LLC d/b/a XFINITY and CITRIX SYSTEMS,
INC.,

Defendants.

Case No. 2:24-cv-68

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Plaintiffs Patricia Andros and Ronald Simmont (“Plaintiffs”), individually and on behalf of all others similarly situated, brings this action against Defendants Comcast Cable Communications, LLC d/b/a Xfinity (“Xfinity”) and Citrix Systems, Inc. (“Citrix”) (collectively, “Defendants”) and alleges as follows based on personal knowledge as to their own acts and on investigation conducted by counsel as to all other allegations:

PARTIES

1. Plaintiff Patricia Andros is a citizen and resident of Pennsylvania.
2. Plaintiff Ronald Simmont is a citizen and resident of Pennsylvania.
3. Defendant Comcast Cable Communications, LLC d/b/a Xfinity is a Delaware limited liability company with its principal place of business in Philadelphia, Pennsylvania.
4. Defendant Citrix Systems, Inc. is a Delaware corporation with its principal place of business in Fort Lauderdale, Florida.

JURISDICTION AND VENUE

5. This Court has subject-matter jurisdiction pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d) because (1) the matter in controversy exceeds the sum or value of \$5,000,000, exclusive of interest and costs, (2) the action is a class action, (3) there are Class members who are diverse from Defendants, and (4) there are more than 100 Class members.

6. This Court has general personal jurisdiction over Defendant Comcast Cable Communications, LLC d/b/a Xfinity because Defendant is a resident of this state.

7. This Court has personal jurisdiction over Defendant Citrix Systems, Inc. because Plaintiffs' claims arise out of Defendant's contacts with this state, and Defendant's contact with this state are substantial.

8. Venue is proper in this district pursuant to 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in this district.

FACTUAL ALLEGATIONS

I. Background

9. Xfinity is based in Philadelphia, Pennsylvania and provides cable television, phone, and internet services to approximately 32 million customers across the United States.

10. Citrix is based in Fort Lauderdale, Florida and provides cloud computing and virtualization services throughout the United States.

11. Defendants' customers, like Plaintiffs and Class members, provided certain Personal Identifying Information ("PII" or "Private Information") to Defendants, which is necessary to obtain Defendants' services.

12. Xfinity uses Citrix services, which requires Xfinity to transfer Plaintiffs' and Class members' Private Information to Citrix.

13. Large companies like Defendants have an acute interest in maintaining the confidentiality of the Private Information entrusted to it, and they are well-aware of the numerous data breaches that have occurred throughout the United States and their responsibility for safeguarding Private Information in their possession.

14. Defendants represented to consumers and the public that they possess robust security features to protect Private Information and that they take their responsibility to protect Private Information seriously.

15. Xfinity's Privacy Policy states:

We know you care about your privacy and the protection of your personal information. We also know it is our responsibility to be clear about how we protect your information. We designed this Privacy Policy to do just that. It explains the types of personal information we collect, and how we collect, use, maintain, protect, and share this information. This Privacy Policy also tells you about the rights and choices you may have when it comes to your personal information.

...

To provide you with our Services, we collect your personal information. This can include information that does not personally identify you - such as device numbers, IP addresses, and account numbers. It may also include information that does personally identify you, such as your name, address, and telephone number. We call any information that identifies you "personally identifiable information" or "PII."

...

If we share your personal information with other companies for their own marketing and advertising activities, we will first get your consent.

...

We follow industry-standard practices to secure the information we collect to prevent the unauthorized access, use, or disclosure of any personal information we collect and maintain. These security

practices include technical, administrative, and physical safeguards, which may vary, depending on the type and sensitivity of the information. Although we take the responsibility of safeguarding your personal information seriously, no security measures are 100% effective and we cannot guarantee that these practices will prevent every unauthorized attempt to access, use, or disclose your information. Comcast also takes additional steps to increase the security and reliability of customer communications. We do not read your outgoing or incoming email, file attachments, video mail, private chat, or instant messages. However, we (along with our service providers) use software and hardware tools to help prevent and block "spam" emails, viruses, spyware, and other harmful or unwanted communications and programs from being sent and received over Comcast.net email and the Comcast Services. To help protect you and the Services against these harmful or unwanted communications and programs, these tools may automatically scan your emails, video mails, instant messages, file attachments, and other files and communications. We do not use these tools for marketing or advertising.¹

16. Citrix's privacy policy states:

Cloud Software Group, Inc. and its subsidiaries ("Cloud Software Group"), respect your concerns about privacy.

...

This Privacy Policy describes the types of personal information we obtain, how we may use that personal information, with whom we may share it and how you may exercise your rights regarding our processing of that information. The Privacy Policy also describes the measures we take to safeguard the personal information we obtain and how you can contact us about our privacy practices.

...

We do not sell or otherwise disclose personal information about you except as described here or at the time of collection.

...

We maintain administrative, technical and physical safeguards, consistent with legal requirements where the personal information was obtained, designed to protect against unlawful or unauthorized

¹ <https://www.xfinity.com/privacy/policy>

destruction, loss, alteration, use or disclosure of, or access to, the personal information provided to us through the Channels.²

17. Citrix further states in their Data Processing Addendum:

We shall implement and maintain appropriate administrative, technical, and organizational practices designed to protect Personal Data against any misuse or accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data. Such security practices are set forth in the Cloud SG Security Exhibit, which is available at <https://www.cloud.com/trust-center/citrix-services-security-exhibit>. We seek to continually strengthen and improve its security practices, and so reserve the right to modify the controls described herein. Any modifications will not diminish the level of security during the relevant term of Products and/or Services. Our employees are bound by appropriate confidentiality agreements and required to take regular data protection training as well as comply with Our corporate privacy and security policies and procedures.³

II. The Data Breach

18. According to Xfinity, on October 10, 2023, Xfinity learned that a vulnerability in Citrix's computer networks was exploited ("Data Breach").

19. Defendants provided further information via a press release:

What Happened? On October 10, 2023, one of Xfinity's software providers, Citrix, announced a vulnerability in one of its products used by Xfinity and thousands of other companies worldwide. At the time Citrix made this announcement, it released a patch to fix the vulnerability. Citrix issued additional mitigation guidance on October 23, 2023. We promptly patched and mitigated our systems.

However, we subsequently discovered that prior to mitigation, between October 16 and October 19, 2023, there was unauthorized access to some of our internal systems that we concluded was a result of this vulnerability. We notified federal law enforcement and conducted an investigation into the nature and scope of the incident. On November 16, 2023, it was determined that information was likely acquired.

² <https://www.cloud.com/privacy-policy>

³ <https://www.cloud.com/content/dam/cloud/documents/legal/cloud-software-group-data-processing-addendum-oct-2023.pdf>

What Information Was Involved? On December 6, 2023, we concluded that the information included usernames and hashed passwords. For some customers, other information was also included, such as names, contact information, last four digits of social security numbers, dates of birth and/or secret questions and answers. However, our data analysis is continuing, and we will provide additional notices as appropriate.

What We Are Doing. To protect your account, we have proactively asked you to reset your password. The next time you login to your Xfinity account, you will be prompted to change your password, if you haven't been asked to do so already.⁴

20. The Data Breach compromised customers' usernames and hashed passwords. For some customers, other information was also included, such as names, contact information, last four digits of social security numbers,⁵ dates of birth and/or secret questions and answers.

21. The Data Breach affected over 35 million customers, including Plaintiffs and Class members, who entrusted their Private Information to Defendants.⁶

22. Defendants sent a breach notification letter to affected customers on or around December 18, 2023.

23. Defendants did not state why they were unable to prevent the Data Breach or which security feature failed.

24. Defendants did not state why they waited over two months after discovering the Data Breach before notifying affected customers.

⁴ <https://assets.xfinity.com/assets/dotcom/learn/Data-Incident1.pdf>

⁵ Even with just the last four digits of a person's Social Security Number, cyber criminals can steal their identity. "When someone wants to steal the identity of a person, they will do whatever it takes to do it. So, only having the last four digits is not going to stop them. They can even use those digits to take your identity away... Because of this, in certain states, there are some limitations regarding how companies can use your SSN. In places like Rhode Island, for instance, you will not be asked for your last four digits." <https://www.stilt.com/immigrants/last-4-digits-of-an-ssn/>.

⁶ <https://apps.web.maine.gov/online/aeviewer/ME/40/49e711c6-e27c-4340-867c-9a529ab3ca2c.shtml>

25. Defendants failed to prevent the Data Breach because they did not adhere to commonly accepted security standards and failed to detect that their databases were subject to a security breach.

III. Plaintiffs' Experience

A. Patricia Andros

26. Plaintiff Patricia Andros is an Xfinity customer and subscribes to Xfinity phone, cable, and internet.

27. Plaintiff learned of the Data Breach from the news. When she went to log in to her Xfinity account, the website prompted her to change her password.

28. Plaintiff is very careful about sharing their sensitive Private Information and diligently maintains her Private Information in a safe and secure manner. Plaintiff has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

29. As a result of the Data Breach, Plaintiff has and will continue to spend time trying to mitigate the consequences of the Data Breach. This includes time spent verifying the legitimacy of communications related to the Data Breach, and self-monitoring her accounts and credit reports to ensure no fraudulent activity has occurred.

30. Plaintiff suffered lost time, annoyance, interference, and inconvenience because of the Data Breach and has anxiety and increased concerns for the loss of her privacy.

31. This time has been lost forever and cannot be recaptured. The harm caused to Plaintiff cannot be undone.

32. Plaintiff further suffered actual injury in the form of damages to and diminution in the value of her Private Information—a form of intangible property that Plaintiff entrusted to Defendants, which was compromised in and as a result of the Data Breach.

33. Plaintiff has suffered imminent and impending injury arising from the present and ongoing risk of fraud, identity theft, and misuse resulting from her Private Information being placed in the hands of cybercriminals.

34. Future identity theft monitoring is reasonable and necessary and such services will include future costs and expenses.

35. Plaintiff has a continuing interest in ensuring that their Private Information, which, upon information and belief, remains in Defendants' control, is protected, and safeguarded from future breaches.

B. Ronald Simmont

36. Plaintiff Ronald Simmont is an Xfinity customer and subscribes to Xfinity cable and internet.

37. Following the Data Breach Xfinity required Plaintiff to log into his account and change his password. When he went to log in to his Xfinity account to change the password, Plaintiff learned of the breach.

38. Plaintiff is very careful about sharing their sensitive Private Information and diligently maintains his Private Information in a safe and secure manner. Plaintiff has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

39. As a result of the Data Breach, Plaintiff has and will continue to spend time trying to mitigate the consequences of the Data Breach. This includes time spent verifying the legitimacy

of communications related to the Data Breach, and self-monitoring his accounts and credit reports to ensure no fraudulent activity has occurred.

40. Plaintiff suffered lost time, annoyance, interference, and inconvenience because of the Data Breach and has anxiety and increased concerns for the loss of his privacy.

41. This time has been lost forever and cannot be recaptured. The harm caused to Plaintiff cannot be undone.

42. Plaintiff further suffered actual injury in the form of damages to and diminution in the value of his Private Information—a form of intangible property that Plaintiff entrusted to Defendants, which was compromised in and as a result of the Data Breach.

43. Plaintiff has suffered imminent and impending injury arising from the present and ongoing risk of fraud, identity theft, and misuse resulting from his Private Information being placed in the hands of cybercriminals.

44. Future identity theft monitoring is reasonable and necessary and such services will include future costs and expenses.

45. Plaintiff has a continuing interest in ensuring that their Private Information, which, upon information and belief, remains in Defendants' control, is protected, and safeguarded from future breaches.

IV. Injuries to Plaintiffs and Class members

46. As a direct and proximate result of Defendants' actions and omissions in failing to protect Plaintiffs and Class members' Private Information, Plaintiffs and Class members have been injured.

47. Plaintiffs and Class members have been placed at a substantial risk of harm in the form of credit fraud or identity theft and have incurred and will likely incur additional damages,

including spending substantial amounts of time monitoring accounts and records, in order to prevent and mitigate credit fraud, identity theft, and financial fraud.

48. In addition to the irreparable damage that may result from the theft of Private Information, identity theft victims must spend numerous hours and their own money repairing the impacts caused by a breach. After conducting a study, the Department of Justice's Bureau of Justice Statistics found that identity theft victims "reported spending an average of about 7 hours clearing up the issues" and resolving the consequences of fraud in 2014.⁷

49. In addition to fraudulent charges and damage to their credit, Plaintiffs and Class members may spend substantial time and expense (a) monitoring their accounts to identify fraudulent or suspicious charges; (b) cancelling and reissuing cards; (c) purchasing credit monitoring and identity theft prevention services; (d) attempting to withdraw funds linked to compromised, frozen accounts; (e) removing withdrawal and purchase limits on compromised accounts; (f) communicating with financial institutions to dispute fraudulent charges; (g) resetting automatic billing instructions and changing passwords; (h) freezing and unfreezing credit bureau account information; (i) cancelling and re-setting automatic payments as necessary; and (j) paying late fees and declined payment penalties as a result of failed automatic payments.

50. Additionally, Plaintiffs and Class members have suffered or are at increased risk of suffering from, *inter alia*, the loss of the opportunity to control how their Private Information is used, the diminution in the value or use of their Private Information, and the loss of privacy.

V. Securing Private Information and Preventing Breaches

51. Defendants could have prevented this Data Breach by properly securing and encrypting the Private Information of Plaintiffs and Class members. Alternatively, Defendants

⁷ U.S. Dep't of Justice, *Victims of Identity Theft, 2014* (Nov. 13, 2017), <http://www.bjs.gov/content/pub/pdf/vit14.pdf>.

could have destroyed the data they no longer had a reasonable need to maintain or only stored data in an Internet-accessible environment when there was a reasonable need to do so.

52. Defendants' negligence in safeguarding the Private Information of Plaintiffs and Class members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

53. Despite the prevalence of public announcements of data breach and data security compromises, Defendants failed to take appropriate steps to protect the Private Information of Plaintiffs and Class members from being compromised.

54. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."⁸ The FTC describes "identifying 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."⁹

55. The ramifications of Defendants' failure to keep secure the Private Information of Plaintiffs and Class members are long lasting and severe. Once Private Information is stolen, particularly Social Security numbers, fraudulent use of that information and damage to victims may continue for years.

VI. The Value of Private Information

56. It is well known that Private Information, and social security numbers and financial account information in particular, is an invaluable commodity and a frequent target of hackers.

⁸ 17 C.F.R. § 248.201 (2013).

⁹ *Id.*

57. People place a high value not only on their Private Information, but also on the privacy of that data. This is because identity theft causes “significant negative financial impact on victims” as well as severe distress and other strong emotions and physical reactions.¹⁰

58. People are particularly concerned with protecting the privacy of their financial account information and social security numbers, which are the “secret sauce” that is “as good as your DNA to hackers.”¹¹ There are long-term consequences to data breach victims whose social security numbers are taken and used by hackers. Even if they know their social security numbers have been accessed, Plaintiffs and Class members cannot obtain new numbers unless they become a victim of social security number misuse. Even then, the Social Security Administration has warned that “a new number probably won’t solve all [] problems . . . and won’t guarantee . . . a fresh start.”¹²

59. The Private Information 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, and bank details have a price range of \$50 to \$200.¹³ Experian reports that a stolen credit or debit card number can sell for \$5 to \$110 on the dark web.¹⁴ Criminals can also purchase access to entire company data breaches from \$900 to \$4,500.¹⁵

¹⁰ Identity Theft Resource Center, *Identity Theft: The Aftermath 2017*,

https://www.ftc.gov/system/files/documents/public_comments/2017/10/00004-141444.pdf.

¹¹ Cameron Huddleston, *How to Protect Your Kids From the Anthem Data Breach*, Kiplinger, (Feb. 10, 2015), <https://www.kiplinger.com/article/credit/T048-C011-S001-how-to-protect-your-kids-from-the-anthem-data-brea.html>.

¹² Social Security Admin., *Identity Theft and Your Social Security Number*, at 6-7, <https://www.ssa.gov/pubs/EN-05-10064.pdf>.

¹³ *Your personal data is for sale on the dark web. Here’s how much it costs*, Digital Trends, Oct. 16, 2019, <https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/>.

¹⁴ *Here’s How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, <https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/>.

¹⁵ *In the Dark*, VPNOverview, 2019, <https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/>.

60. 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.¹⁶

61. 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.

62. 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."¹⁷

¹⁶ Social Security Administration, *Identity Theft and Your Social Security Number*, <https://www.ssa.gov/pubs/EN-05-10064.pdf>.

¹⁷ Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), <http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft>.

63. 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. The information compromised in this Data Breach is impossible to “close” and difficult, if not impossible, to change.

64. 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.”¹⁸

65. 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.

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

67. There may be a time lag between when harm occurs versus when it is discovered, and also between when Private Information 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 have 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.¹⁹

¹⁸ Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), <https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html>.

¹⁹ *Report to Congressional Requesters*, GAO, at 29 (June 2007), <https://www.gao.gov/assets/gao-07-737.pdf>.

68. At all relevant times, Defendants knew, or reasonably should have known, of the importance of safeguarding the Private Information of Plaintiffs and Class members, including Social Security numbers, and of the foreseeable consequences that would occur if their data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiffs and Class members as a result of a breach.

69. Plaintiffs and Class members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. Plaintiffs and Class members are incurring and will continue to incur such damages in addition to any fraudulent use of their Private Information.

70. Defendants knew of the unique type and the significant volume of data contained in the Private Information that Defendants stored on their networks, and, thus, the significant number of individuals who would be harmed by the exposure of the data.

71. The injuries to Plaintiffs and Class members were directly and proximately caused by Defendants' failure to implement or maintain adequate data security measures for the Private Information of Plaintiffs and Class members.

VII. Industry Standards for Data Security

72. As explained by the Federal Bureau of Investigation, “[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection.”²⁰

73. In light of the numerous high-profile data breaches targeting companies like Target, Neiman Marcus, eBay, Anthem, Deloitte, Equifax, Marriott, T-Mobile, and Capital One, Defendants knew of the importance of safeguarding Private Information, as well as of the foreseeable consequences of its systems being breached.

²⁰ *How to Protect Your Networks from Ransomware*, FBI, <https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view>.

74. Therefore, the increase in such attacks, and the attendant risk of future attacks, were widely known to the public and to anyone in Defendants' industry, including Defendants.

75. Security standards commonly accepted among businesses that store Private Information using the internet include, without limitation:

- a. Maintaining a secure firewall configuration;
- b. Monitoring for suspicious or irregular traffic to servers;
- c. Monitoring for suspicious credentials used to access servers;
- d. Monitoring for suspicious or irregular activity by known users;
- e. Monitoring for suspicious or unknown users;
- f. Monitoring for suspicious or irregular server requests;
- g. Monitoring for server requests for Private Information;
- h. Monitoring for server requests from VPNs; and
- i. Monitoring for server requests from Tor exit nodes.

76. The U.S. Federal Trade Commission ("FTC") publishes guides for businesses for cybersecurity²¹ and protection of Private Information²² which includes basic security standards applicable to all types of businesses.

77. The FTC recommends that businesses:

- a. Identify all connections to the computers where you store sensitive information.
- b. Assess the vulnerability of each connection to commonly known or reasonably foreseeable attacks.

²¹ Start with Security: A Guide for Business, FTC (June 2015), <https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf>.

²² Protecting Personal Information: A Guide for Business, FTC (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting_personalinformation.pdf.

- c. Do not store sensitive consumer data on any computer with an internet connection unless it is essential for conducting their business.
- d. Scan computers on their network to identify and profile the operating system and open network services. If services are not needed, they should be disabled to prevent hacks or other potential security problems. For example, if email service or an internet connection is not necessary on a certain computer, a business should consider closing the ports to those services on that computer to prevent unauthorized access to that machine.
- e. Pay particular attention to the security of their web applications—the software used to give information to visitors to their websites and to retrieve information from them. Web applications may be particularly vulnerable to a variety of hacker attacks.
- f. Use a firewall to protect their computers from hacker attacks while it is connected to a network, especially the internet.
- g. Determine whether a border firewall should be installed where the business's network connects to the internet. A border firewall separates the network from the internet and may prevent an attacker from gaining access to a computer on the network where sensitive information is stored. Set access controls—settings that determine which devices and traffic get through the firewall—to allow only trusted devices with a legitimate business need to access the network. Since the protection a firewall provides is only as effective as its access controls, they should be reviewed periodically.
- h. Monitor incoming traffic for signs that someone is trying to hack in. Keep an eye out for activity from new users, multiple log-in attempts from unknown users or computers, and higher-than-average traffic at unusual times of the day.
- i. Monitor outgoing traffic for signs of a data breach. Watch for unexpectedly large amounts of data being transmitted from their system to an unknown user. If large amounts of information are being transmitted from a business' network, the transmission should be investigated to make sure it is authorized.

78. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer information, 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, 15 U.S.C.

§ 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.²³

79. Because Plaintiffs and Class members entrusted Defendants with Private Information, Defendants had a duty to keep the Private Information secure.

80. Plaintiffs and Class members reasonably expect that when their Private Information is provided to a sophisticated business for a specific purpose, that business will safeguard their Private Information and use it only for that purpose.

81. Nonetheless, Defendants failed to prevent the Data Breach. Had Defendants properly maintained and adequately protected their systems, they could have prevented the Data Breach.

CLASS ALLEGATIONS

82. This action is brought as a class action pursuant to Fed. R. Civ. P. 23.

83. The Class is defined as follows:

Nationwide Class: All persons whose Private Information was maintained on Defendants' servers that were compromised in the Data Breach.

Pennsylvania Subclass: All persons in Pennsylvania whose Private Information was maintained on Defendants' servers that were compromised in the Data Breach.

84. The Class excludes the following: Defendants, their affiliates, and their current and former employees, officers and directors, and the Judge assigned to this case.

85. The Class definition may be modified, changed, or expanded based upon discovery and further investigation.

²³ Federal Trade Commission, *Privacy and Security Enforcement: Press Releases*, <https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement>.

86. *Numerosity*: The Class is so numerous that joinder of all members is impracticable, evidenced by the tens of millions of individuals presently known to have been injured by Defendants' conduct. The Class is ascertainable by records in the possession of Defendants or third parties.

87. *Commonality*: Questions of law or fact common to the Class include, without limitation:

- a. Whether Defendants owed a duty or duties to Plaintiffs and Class members to exercise due care in collecting, storing, safeguarding, and obtaining their Private Information;
- b. Whether Defendants breached that duty or those duties;
- c. Whether Defendants failed to establish appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of records to protect against known and anticipated threats to security;
- d. Whether the security provided by Defendants was satisfactory to protect Private Information as compared to industry standards;
- e. Whether Defendants misrepresented or failed to provide adequate information regarding the type of security practices used;
- f. Whether Defendants knew or should have known that they did not employ reasonable measures to keep Plaintiffs and Class members' Private Information secure and prevent loss or misuse of that Private Information;
- g. Whether Defendants acted negligently in connection with the monitoring and protecting of Plaintiffs and Class members' Private Information;
- h. Whether Defendants' conduct was intentional, willful, or negligent;
- i. Whether Plaintiffs and Class members suffered damages as a result of Defendants' conduct, omissions, or misrepresentations; and
- j. Whether Plaintiffs and Class members are entitled to injunctive, declarative, and monetary relief as a result of Defendants' conduct.

88. *Typicality*: Plaintiffs' claims are typical of the claims of Class members. Plaintiffs and Class members were injured and suffered damages in substantially the same manner, have the

same claims against Defendants relating to the same course of conduct, and are entitled to relief under the same legal theories.

89. *Adequacy*: Plaintiffs will fairly and adequately protect the interests of the Class and have no interests antagonistic to those of the Class. Plaintiffs' counsel are experienced in the prosecution of complex class actions, including data breach actions with issues, claims, and defenses similar to the present case.

90. *Predominance and superiority*: Questions of law or fact common to Class members predominate over any questions affecting individual members. A class action is superior to other available methods for the fair and efficient adjudication of this case because individual joinder of all Class members is impracticable and the amount at issue for each Class member would not justify the cost of litigating individual claims. Should individual Class members be required to bring separate actions, this Court would be confronted with a multiplicity of lawsuits burdening the court system while also creating the risk of inconsistent rulings and contradictory judgments. In contrast to proceeding on a case-by-case basis, in which inconsistent results will magnify the delay and expense to all parties and the court system, this class action presents far fewer management difficulties while providing unitary adjudication, economies of scale and comprehensive supervision by a single court. There are no known difficulties that are likely to be encountered in the management of this action that would preclude its maintenance as a class action.

91. Accordingly, this class action may be maintained pursuant to Fed. R. Civ. P. 23(b)(3).

92. Defendants' unlawful conduct applies generally to all Class members, thereby making appropriate final equitable relief with respect to the Class as a whole.

93. Accordingly, this class action may be maintained pursuant to Fed. R. Civ. P. 23(b)(2).

CAUSES OF ACTION

COUNT I
NEGLIGENCE

(on behalf of the Class against all Defendants)

94. All preceding paragraphs are incorporated herein by reference as though fully set forth herein.

95. Defendants owed a duty of care to Plaintiffs and Class members to use reasonable means to secure and safeguard the entrusted Private Information, to prevent its unauthorized access and disclosure, to guard it from theft, and to detect any attempted or actual breach of its systems. These common law duties existed because Plaintiffs and Class members were the foreseeable and probable victims of any inadequate security practices. In fact, not only was it foreseeable that Plaintiffs and Class members would be harmed by the failure to protect their Private Information because hackers routinely attempt to steal such information and use it for nefarious purposes, but Defendants knew that it was more likely than not Plaintiffs and Class members would be harmed by such exposure of their Private Information.

96. Defendants' duties to use reasonable security measures also arose as a result of the special relationship that existed between Defendants, on the one hand, and Plaintiffs and Class members, on the other hand. The special relationship arose because Plaintiffs and Class members entrusted their Private Information with Defendants, Defendants accepted and held the Private Information, and Defendants represented that the Private Information would be kept secure pursuant to their data security policies. Defendants could have ensured that their data security systems and practices were sufficient to prevent or minimize the data breach.

97. Defendants' duties to use reasonable data security measures also arose under Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect Private Information. Various FTC publications and data security breach orders further form the basis of Defendants' duties. In addition, individual states have enacted statutes based upon the FTC Act that also created a duty.

98. Defendants' violations of Section 5 of the FTC Act constitute negligence per se.

99. Defendants breached the aforementioned duties when they failed to use security practices that would protect Plaintiffs and Class members' Private Information, thus resulting in unauthorized third-party access to the Plaintiffs and Class members' Private Information.

100. Defendants further breached the aforementioned duties by failing to design, adopt, implement, control, manage, monitor, update, and audit their processes, controls, policies, procedures, and protocols to comply with the applicable laws and safeguard and protect Plaintiffs and Class members' Private Information within their possession, custody, and control.

101. As a direct and proximate cause of failing to use appropriate security practices, Plaintiffs and Class members' Private Information was disseminated and made available to unauthorized third parties.

102. Defendants admitted that Plaintiffs and Class members' Private Information was wrongfully disclosed as a result of the breach.

103. The breach caused direct and substantial damages to Plaintiffs and Class members, as well as the possibility of future and imminent harm through the dissemination of their Private Information and the greatly enhanced risk of credit fraud or identity theft.

104. By engaging in the forgoing acts and omissions, Defendants committed the common law tort of negligence. For all the reasons stated above, Defendants' conduct was negligent and departed from reasonable standards of care including by, but not limited to: failing to adequately protect the Private Information; failing to conduct regular security audits; and failing to provide adequate and appropriate supervision of persons having access to Plaintiffs and Class members' Private Information.

105. But for Defendants' wrongful and negligent breach of its duties owed to Plaintiffs and Class members, their Private Information would not have been compromised.

106. Neither Plaintiffs nor the Class contributed to the breach or subsequent misuse of their Private Information as described in this Complaint.

107. As a direct and proximate result of Defendants' actions and inactions, Plaintiffs and Class members have been put at an increased risk of credit fraud or identity theft, and Defendants must mitigate damages by providing adequate credit and identity monitoring services.

108. Plaintiffs and Class members are entitled to damages for the reasonable costs of future credit and identity monitoring services for a reasonable period of time, substantially in excess of one year.

109. Plaintiffs and Class members are entitled to damages to the extent that they have directly sustained damages as a result of identity theft or other unauthorized use of their Private Information, including the amount of time Plaintiffs and Class members have spent and will continue to spend as a result of Defendants' negligence.

110. Plaintiffs and Class members are entitled to damages to the extent their Private Information has been diminished in value because Plaintiffs and Class members no longer control their Private Information and to whom it is disseminated.

COUNT II
BREACH OF IMPLIED CONTRACT
(on behalf of the Class against all Defendants)

111. Plaintiffs hereby incorporates by reference all preceding paragraphs as though fully set forth herein.

112. Defendants invited Plaintiffs and Class members to provide their Private Information to Defendants. As consideration for the benefits Defendants provided, Plaintiffs and Class members provided their Private Information to Defendants. When Plaintiffs and Class members provided their Private Information to Defendants, they entered into implied contracts by which Defendants agreed to protect their Private Information and only use it solely to administer benefits. As part of the offer, Defendants would safeguard the Private Information using reasonable or industry-standard means.

113. Accordingly, Plaintiffs and Class members accepted Defendants' offer to administer benefits and provided Defendants their Private Information.

114. Plaintiffs and Class members fully performed their obligations under the implied contracts with Defendants. However, Defendants breached the implied contracts by failing to safeguard Plaintiffs' and the Class's Private Information.

115. The losses and damages Plaintiffs and Class members sustained that are described herein were the direct and proximate result of Defendants' breaches of its implied contracts with them. Additionally, because Plaintiffs and Class members continue to be parties to the ongoing administration and distribution of benefits under the contracts, and because damages may not provide a complete remedy for the breaches alleged herein, Plaintiffs and Class members are therefore entitled to specific performance of the contracts to ensure data security measures necessary to properly effectuate the contracts maintain the security of their Private Information from unlawful exposure.

116. Defendants' conduct as alleged herein also violated the implied covenant of good faith and fair dealing inherent in every contract, and Plaintiffs and Class members are entitled to associated damages and specific performance.

COUNT III
BREACH OF THIRD-PARTY BENEFICIARY CONTRACT
(on behalf of the Class against Defendant Citrix)

117. All preceding paragraphs are incorporated herein by reference as though fully set forth herein.

118. Citrix entered into contracts with its clients, including Xfinity, to provide cloud computing and virtualization services.

119. Citrix's services included data security practices, procedures, and protocols sufficient to safeguard the Private Information that was entrusted to it.

120. Such contracts were made expressly for the benefit of Plaintiffs and Class members, as it was their Private Information that Citrix agreed to receive, store, utilize, transfer, and protect through its services. Thus, the benefit of collection and protection of the Private Information belonging to Plaintiffs and Class members was the direct and primary objective of the contracting parties and Plaintiffs and Class members were direct and express beneficiaries of such contracts.

121. Citrix knew or should have known that if it were to breach these contracts with its customers, Plaintiffs and Class members would be harmed.

122. Citrix breached their contracts with customers by, among other things, failing to adequately secure Plaintiffs and Class members' Private Information, and, as a result, Plaintiffs and Class members were harmed by Citrix's failure to secure their Private Information.

123. As a direct and proximate result of Citrix's breach, Plaintiffs and Class members are at a current and ongoing risk of identity theft, and Plaintiffs and Class members sustained incidental and consequential damages including: (i) financial "out-of-pocket" costs incurred

mitigating the materialized risk and imminent threat of identity theft; (ii) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (iii) financial “out-of-pocket” costs incurred due to actual identity theft; (iv) loss of time incurred due to actual identity theft; (v) loss of time due to increased spam and targeted marketing emails; (vi) diminution of value of their Private Information; (vii) future costs of identity theft monitoring; (viii) and the continued risk to their Private Information, which remains in Citrix’s control, and which is subject to further breaches, so long as Citrix fails to undertake appropriate and adequate measures to protect Plaintiffs and Class members’ Private Information.

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

COUNT IV
UNJUST ENRICHMENT
(on behalf of the Class against all Defendants)

125. All preceding paragraphs are incorporated herein by reference as though fully set forth herein.

126. Plaintiffs and Class members have an interest, both equitable and legal, in their Private Information that was conferred upon, collected by, and maintained by Defendants and that was ultimately compromised in the data breach.

127. Defendants, by way of their acts and omissions, knowingly and deliberately enriched themselves by saving the costs they reasonably should have expended on security measures to secure Plaintiffs and Class members’ Private Information.

128. Defendants also understood and appreciated that the Private Information pertaining to Plaintiffs and Class members was private and confidential and its value depended upon Defendants maintaining the privacy and confidentiality of that Private Information.

129. Instead of providing for a reasonable level of security that would have prevented the breach—as is common practice among companies entrusted with such Private Information—Defendants instead consciously and opportunistically calculated to increase their own profits at the expense of Plaintiffs and Class members. Nevertheless, Defendants continued to obtain the benefits conferred on them by Plaintiffs and Class members. The benefits conferred upon, received, and enjoyed by Defendants were not conferred gratuitously, and it would be inequitable and unjust for Defendants to retain these benefits.

130. Plaintiffs and Class members, on the other hand, suffered as a direct and proximate result. As a result of Defendants' decision to profit rather than provide requisite security, and the resulting breach disclosing Plaintiffs and Class members' Private Information, Plaintiffs and Class members suffered and continue to suffer considerable injuries in the forms of, *inter alia*, attempted identity theft, time and expenses mitigating harms, diminished value of Private Information, loss of privacy, and increased risk of harm.

131. Thus, Defendants engaged in opportunistic conduct in spite of its duties to Plaintiffs and Class members, wherein they profited from interference with Plaintiffs and Class members' legally protected interests. As such, it would be inequitable, unconscionable, and unlawful to permit Defendants to retain the benefits it derived as a consequence of its conduct.

132. Accordingly, Plaintiffs and Class members respectfully request that this Court award relief in the form of restitution or disgorgement in the amount of the benefit conferred on Defendants as a result of their wrongful conduct, including specifically, the amounts that Defendants should have spent to provide reasonable and adequate data security to protect Plaintiffs and Class members' Private Information, and compensatory damages.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs prays for a judgment as follows:

- a. For an order certifying the Class, appointing Plaintiffs as Class Representative, and appointing the law firms representing Plaintiffs as counsel for the Class;
- b. For compensatory, punitive, statutory, and treble damages in an amount to be determined at trial;
- c. Payment of costs and expenses of suit herein incurred;
- d. Both pre-and post-judgment interest on any amounts awarded;
- e. Payment of reasonable attorneys' fees and expert fees;
- f. Such other and further relief as the Court may deem proper.

JURY DEMAND

Trial by jury is demanded.

Dated: January 5, 2024

Respectfully submitted,

/s/Charles E. Schaffer

Charles E. Schaffer
Nicholas J. Elia
LEVIN SEDRAN & BERMAN LLP
510 Walnut Street, Suite 500
Philadelphia, PA 19106
Phone: (215) 592-1500
cschaffer@lfsblaw.com
nelia@lfsblaw.com

Jeffrey S. Goldenberg *
Todd B. Naylor *
GOLDENBERG SCHNEIDER, LPA
4445 Lake Forest Drive, Suite 490
Cincinnati, Ohio 45242
Phone: (513) 345-8291
Facsimile: (513) 345-8294
jgoldenberg@gs-legal.com
tnaylor@gs-legal.com

Jeffrey K. Brown, Esq.
Andrew Costello, Esq.
LEEDS BROWN LAW, P.C
One Old Country Road, Suite 347
Carle Place, NY 11514
Tel: (516) 873-9550
jbrown@leedsbrownlaw.com
acostello@leedsbrownlaw.com

Counsel for Plaintiffs and Proposed Class

** Pro hac vice forthcoming*

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
(b) County of Residence of First Listed Plaintiff
(c) Attorneys (Firm Name, Address, and Telephone Number)

DEFENDANTS
County of Residence of First Listed Defendant
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
2 U.S. Government Defendant
3 Federal Question (U.S. Government Not a Party)
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)
PTF DEF
Citizen of This State 1 1
Citizen of Another State 2 2
Citizen or Subject of a Foreign Country 3 3
Incorporated or Principal Place of Business In This State 4 4
Incorporated and Principal Place of Business In Another State 5 5
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
TORTS: PERSONAL INJURY: 310 Airplane, 315 Airplane Product Liability, 320 Assault, Libel & Slander, 330 Federal Employers' Liability, 340 Marine, 345 Marine Product Liability, 350 Motor Vehicle, 355 Motor Vehicle Product Liability, 360 Other Personal Injury, 362 Personal Injury - Medical Malpractice; PERSONAL INJURY: 365 Personal Injury - Product Liability, 367 Health Care/Pharmaceutical Personal Injury Product Liability, 368 Asbestos Personal Injury Product Liability; PERSONAL PROPERTY: 370 Other Fraud, 371 Truth in Lending, 380 Other Personal Property Damage, 385 Property Damage Product Liability
FORFEITURE/PENALTY: 625 Drug Related Seizure of Property 21 USC 881, 690 Other
LABOR: 710 Fair Labor Standards Act, 720 Labor/Management Relations, 740 Railway Labor Act, 751 Family and Medical Leave Act, 790 Other Labor Litigation, 791 Employee Retirement Income Security Act
IMMIGRATION: 462 Naturalization Application, 465 Other Immigration Actions
BANKRUPTCY: 422 Appeal 28 USC 158, 423 Withdrawal 28 USC 157
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):
Brief description of cause:

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 SIGNATURE OF ATTORNEY OF RECORD

FOR OFFICE USE ONLY
RECEIPT # AMOUNT APPLYING IFP JUDGE MAG. JUDGE

INSTRUCTIONS FOR ATTORNEYS COMPLETING CIVIL COVER SHEET FORM JS 44

Authority For Civil Cover Sheet

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

- I.(a) Plaintiffs-Defendants.** Enter names (last, first, middle initial) of plaintiff and defendant. If the plaintiff or defendant is a government agency, use only the full name or standard abbreviations. If the plaintiff or defendant is an official within a government agency, identify first the agency and then the official, giving both name and title.
- (b) County of Residence.** For each civil case filed, except U.S. plaintiff cases, enter the name of the county where the first listed plaintiff resides at the time of filing. In U.S. plaintiff cases, enter the name of the county in which the first listed defendant resides at the time of filing. (NOTE: In land condemnation cases, the county of residence of the "defendant" is the location of the tract of land involved.)
- (c) Attorneys.** Enter the firm name, address, telephone number, and attorney of record. If there are several attorneys, list them on an attachment, noting in this section "(see attachment)".
- II. Jurisdiction.** The basis of jurisdiction is set forth under Rule 8(a), F.R.Cv.P., which requires that jurisdictions be shown in pleadings. Place an "X" in one of the boxes. If there is more than one basis of jurisdiction, precedence is given in the order shown below.
 United States plaintiff. (1) Jurisdiction based on 28 U.S.C. 1345 and 1348. Suits by agencies and officers of the United States are included here. United States defendant. (2) When the plaintiff is suing the United States, its officers or agencies, place an "X" in this box.
 Federal question. (3) This refers to suits under 28 U.S.C. 1331, where jurisdiction arises under the Constitution of the United States, an amendment to the Constitution, an act of Congress or a treaty of the United States. In cases where the U.S. is a party, the U.S. plaintiff or defendant code takes precedence, and box 1 or 2 should be marked.
 Diversity of citizenship. (4) This refers to suits under 28 U.S.C. 1332, where parties are citizens of different states. When Box 4 is checked, the citizenship of the different parties must be checked. (See Section III below; **NOTE: federal question actions take precedence over diversity cases.**)
- III. Residence (citizenship) of Principal Parties.** This section of the JS 44 is to be completed if diversity of citizenship was indicated above. Mark this section for each principal party.
- IV. Nature of Suit.** Place an "X" in the appropriate box. If there are multiple nature of suit codes associated with the case, pick the nature of suit code that is most applicable. Click here for: [Nature of Suit Code Descriptions](#).
- V. Origin.** Place an "X" in one of the seven boxes.
 Original Proceedings. (1) Cases which originate in the United States district courts.
 Removed from State Court. (2) Proceedings initiated in state courts may be removed to the district courts under Title 28 U.S.C., Section 1441.
 Remanded from Appellate Court. (3) Check this box for cases remanded to the district court for further action. Use the date of remand as the filing date.
 Reinstated or Reopened. (4) Check this box for cases reinstated or reopened in the district court. Use the reopening date as the filing date.
 Transferred from Another District. (5) For cases transferred under Title 28 U.S.C. Section 1404(a). Do not use this for within district transfers or multidistrict litigation transfers.
 Multidistrict Litigation – Transfer. (6) Check this box when a multidistrict case is transferred into the district under authority of Title 28 U.S.C. Section 1407.
 Multidistrict Litigation – Direct File. (8) Check this box when a multidistrict case is filed in the same district as the Master MDL docket.
PLEASE NOTE THAT THERE IS NOT AN ORIGIN CODE 7. Origin Code 7 was used for historical records and is no longer relevant due to changes in statute.
- VI. Cause of Action.** Report the civil statute directly related to the cause of action and give a brief description of the cause. **Do not cite jurisdictional statutes unless diversity.** Example: U.S. Civil Statute: 47 USC 553 Brief Description: Unauthorized reception of cable service.
- VII. Requested in Complaint.** Class Action. Place an "X" in this box if you are filing a class action under Rule 23, F.R.Cv.P.
 Demand. In this space enter the actual dollar amount being demanded or indicate other demand, such as a preliminary injunction.
 Jury Demand. Check the appropriate box to indicate whether or not a jury is being demanded.
- VIII. Related Cases.** This section of the JS 44 is used to reference related 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.

DESIGNATION FORM

(to be used by counsel or pro se plaintiff to indicate the category of the case for the purpose of assignment to the appropriate calendar)

Address of Plaintiff: _____

Address of Defendant: _____

Place of Accident, Incident or Transaction: _____


RELATED CASE, IF ANY:

Case Number: _____ Judge: _____ Date Terminated: _____

Civil cases are deemed related when **Yes** is answered to any of the following questions:

- 1. Is this case related to property included in an earlier numbered suit pending or within one year previously terminated action in this court? Yes No
- 2. Does this case involve the same issue of fact or grow out of the same transaction as a prior suit pending or within one year previously terminated action in this court? Yes No
- 3. Does this case involve the validity or infringement of a patent already in suit or any earlier numbered case pending or within one year previously terminated action of this court? Yes No
- 4. Is this case a second or successive habeas corpus, social security appeal, or pro se civil rights case filed by the same individual? Yes No

I certify that, to my knowledge, the within case is / is not related to any case now pending or within one year previously terminated action in this court except as noted above.

DATE: _____  _____

Attorney-at-Law / Pro Se Plaintiff

Attorney I.D. # (if applicable)

CIVIL: (Place a ✓ in one category only)

A. Federal Question Cases:

- 1. Indemnity Contract, Marine Contract, and All Other Contracts
- 2. FEELA
- 3. Jones Act-Personal Injury
- 4. Antitrust
- 5. Patent
- 6. Labor-Management Relations
- 7. Civil Rights
- 8. Habeas Corpus
- 9. Securities Act(s) Cases
- 10. Social Security Review Cases
- 11. All other Federal Question Cases
(Please specify): _____

B. Diversity Jurisdiction Cases:


- 1. Insurance Contract and Other Contracts
- 2. Airplane Personal Injury
- 3. Assault, Defamation
- 4. Marine Personal Injury
- 5. Motor Vehicle Personal Injury
- 6. Other Personal Injury (Please specify): _____
- 7. Products Liability
- 8. Products Liability – Asbestos
- 9. All other Diversity Cases
(Please specify): _____

ARBITRATION CERTIFICATION

(The effect of this certification is to remove the case from eligibility for arbitration.)

I, _____, counsel of record or pro se plaintiff, do hereby certify:

- Pursuant to Local Civil Rule 53.2, § 3(c) (2), that to the best of my knowledge and belief, the damages recoverable in this civil action case exceed the sum of \$150,000.00 exclusive of interest and costs:
- Relief other than monetary damages is sought.

DATE: _____  _____

Attorney-at-Law / Pro Se Plaintiff

Attorney I.D. # (if applicable)

NOTE: A trial de novo will be a trial by jury only if there has been compliance with F.R.C.P. 38.