IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
AUSTIN DIVISION

DAVID REZA PIRI	§	
	§	
Plaintiff,	§	
	§	**Civil Action No. 1:18-cv-269**
v.	§	
	§	**Complaint**
	§	
T-MOBILE US, INC., and	§	
T-MOBILE USA, INC.,	§	
	§	
	§	
Defendants.	§	
	§	
	§	
	§	

ORIGINAL COMPLAINT

Plaintiff, David Reza Piri, ("Plaintiff") files this Complaint for breach of contract, negligence, deceptive trade practices, and other claims against Defendants T-Mobile US, Inc., and T-Mobile USA, Inc. ("T-Mobile") on personal knowledge as to all facts and on information and belief as to all other matters, and shall show the Court as follows:

I.
PRELIMINARY STATEMENT

T-Mobile provides mobile telephone and data services to millions of customers in the United States. Plaintiff has been a T-Mobile customer since 2002. As a mobile carrier for Plaintiff, T-Mobile has access to Plaintiff's confidential personal identifying information such as his name, address, social security number, and phone number. According to T-Mobile's terms and conditions, privacy policy, and related representations on its website, T-Mobile does not provide access to this information unless it is to an "Authorized User." Moreover, T-Mobile takes

precautions and security measures to protect this data from outside parties. Despite these promises and representations, T-Mobile has had a security hole in its system for several months that has allowed hackers access to customers', like Plaintiff's, personal confidential information.

On May 10th, 2017, hackers exploited this security breach to obtain Plaintiff's personal confidential information, then used this information via social engineering to impersonate Plaintiff and port his phone number into their possession. The hackers were able to accomplish this despite Plaintiff informing T-Mobile on May 9th, 2017, the day before the hack occurred, that he did not want his number ported and not to authorize the porting of his phone number to a different phone. T-Mobile's granting the hackers access to Plaintiff's confidential personal information was negligent, deceptive, and a breach of the terms of its agreement with Plaintiff. Plaintiff has suffered damages as a result of T-Mobile's misconduct. By this action, Plaintiff seeks to obtain monetary relief to remedy those damages and hold T-Mobile responsible for its improper activities so that the painful injury that Plaintiff suffered does not happen to future customers.

II. THE PARTIES

1. Plaintiff David Reza Piri is an individual and citizen of Texas.

2. Defendant T-Mobile US, Inc. is a Delaware corporation with its principal place of business at 12920 SE 38th Street, Bellevue, Washington 98006. On information and belief, T-Mobile US, Inc. may be served through its registered agent for service, Corporation Service Company, 2711 Centerville Rd Suite 400, Wilmington, Delaware 19808.

3. Defendant T-Mobile USA, Inc. is a Delaware corporation with its principal place of business at 12920 SE 38th Street, Bellevue, Washington 98006, and is a wholly-owned subsidiary of T-Mobile US, Inc. On information and belief, T-Mobile USA, Inc. may be served through its registered agent for service, Corporation Service Company, 211 E. 7th St. Suite 620,

Austin, Texas 78701-3218. On information and belief, Defendant T-Mobile USA, Inc. has a fraud department at 12920 SE 38th Street, Bellevue, Washington 98006.

III. JURISDICTION AND VENUE

4. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1332, because complete diversity exists between the parties and the amount in controversy exceeds $75,000.00.

5. This Court has personal jurisdiction over T-Mobile because it is doing business in Texas and T-Mobile's conduct and connections with Texas are purposeful and such that it must have reasonably foreseen that it could be sued in Texas.

6. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b).

IV. FACTS

7. On May 8th, 2017, Plaintiff's brother, Michael Piri, discovered that his T-Mobile account had been hacked. Two days later, on May 10th, 2017, Plaintiff's personal account had been fully hacked and his digital identity stolen despite his many warnings to T-Mobile of the impending hack and desperate pleas to prevent it.

8. Similar to many of T-Mobile's other 76.9 million customers, much of Plaintiff's data on his T-Mobile account was intimately tied to other service accounts and his business. Via 2 Factor Authorization ("2FA"), the entirety of Plaintiff's digital identity was compromised once his T-Mobile phone number was ported on May 10th, 2017. During the hack, and its aftermath, Plaintiff's work and personal life suffered considerably. Some of it ceased entirely. Moreover, Plaintiff faces an ongoing risk of identity theft for the remainder of his personal and professional life. As recognized by the Senate Commerce Subcommittee on Consumer Protection, the "sensitive nature of the compromised personal data" stolen from Plaintiff is of "particular value to

identity thieves."[1] Thus, Plaintiff remains in a constant state of apprehension because of his greatly increased vulnerability to future thefts of his personal and business identities.

9. T-Mobile has consistently agreed and represented, via its Terms & Conditions and other warranties of security and privacy, respectively, that it shall prevent unauthorized access to customers' personal identifying information and employ the requisite "physical, technical and administrative safeguards"[2] intended to protect a customer's account and personal identifying information. In this respect, T-Mobile has consistently fallen short of its agreements and representations.

10. Thus, Plaintiff asks that the Court declare that T-Mobile, through its negligent, deceptive, and breaching conduct, has monetarily and mentally damaged him and consequently allow him to recover to the full extent permissible under law.

a. T-Mobile Failed to Detect a Security Deficiency Exploited by SIM Swapping Hackers for Months.

11. T-Mobile is no stranger to catastrophic breaches in its security. In 2004, a single hacker obtained access to over 400 T-Mobile customers' personal identifying information for at least seven months.[3] In 2012, hacktivist group TeaMp0isoN obtained and then published the data, names, and passwords of several T-Mobile staff using a common, easy to defend against SQL injection.[4] Then in 2013, T-Mobile customers' data was compromised when hackers obtained

[1] *Blumenthal, Nelson, Schatz, Demand Answers from T-Mobile and Experian Following Security Breach of 15 Million Customers; Personal Data, Including Social Security Numbers*, Blumenthal.Senate.gov, https://www.blumenthal.senate.gov/newsroom/press/release/demand-answers-from-t-mobile-and-experian (last visited Nov. 30, 2017)
[2] *Privacy & Security Resources*, T-Mobile.com, https://www.t-mobile.com/company/privacy-resources/identity-theft.html (last visited Nov. 30, 2017)
[3] *T-Mobile Hack*, https://www.schneier.com/blog/archives/2005/02/tmobile_hack_1.html (last visited Oct. 19, 2017)
[4] *T-Mobile staff data and passwords hacked and published*, https://www.scmagazineuk.com/t-mobile-staff-data-and-passwords-hacked-and-published/article/545419/ (last visited Oct. 19, 2017)

personal identifying information stored on a T-Mobile vendor's system.[5] In 2015, over 15 million T-Mobile customers' personal information was yet again stolen by hackers targeting Experian, a major credit bureau in charge of conducting credit checks on T-Mobile customers.[6] Finally, in 2017, T-Mobile was the target of at least two known hacks. First, in March 2017, a cybersecurity expert expressed to Congress that T-Mobile's Washington, D.C. network may have been compromised by a hacker collecting "massive amounts of location data," monitoring phone calls, or cloning phone numbers.[7,8] Second, hackers once again targeted T-Mobile's substandard security infrastructure by employing common, easily detectable and beatable hacking techniques for months in order to obtain the personal identifying information of potentially up to all 76.9 million T-Mobile customers.[9]

12. This series of known breaches over the course of at least thirteen years highlights a troubling pattern. T-Mobile's security has consistently been egregiously below par. For this, T-Mobile simply has "no excuse," and hackers are right to believe that "T-Mobile has always had terrible security practices" since its inception.[10] T-Mobile is simply not providing the security and

---

[5] *T-Mobile Confirms Hack on Third-Party Vendor Revealed Personal Information*, https://www.technobuffalo.com/2014/01/23/t-mobile-confirms-hack-on-third-party-vendor-revealed-personal-information/ (last visited Oct. 19, 2017)

[6] *T-Mobile customers' info breached after Experian hack*, http://money.cnn.com/2015/10/01/technology/tmobile-experian-data-breach/index.html (last visited Oct. 19, 2017)

[7] *A Security Expert Warned Congress That T-Mobile's DC Cell Network Has Been Hacked*, https://lieu.house.gov/media-center/in-the-news/security-expert-warned-congress-t-mobiles-dc-cell-network-has-been-hacked (last visited Oct. 19, 2017)

[8] *D.C. Cell Network May Have Been Hacked, Used to Monitor Calls*, http://www.ibtimes.com/dc-cell-network-may-have-been-hacked-used-monitor-calls-2510554 (last visited Oct. 19, 2017)

[9] *T-Mobile website bug let hackers steal data with a phone number*, https://www.engadget.com/2017/10/11/t-mobile-website-flaw-social-engineering-hacks/ (last visited Oct. 19, 2017)

[10] *There's 'No Excuse' for the T-Mobile Bug That Helped Hackers Steal Accounts*, https://motherboard.vice.com/en_us/article/7xkyyz/t-mobile-customer-data-bug-hackers-no-excuse (last visited Oct. 19, 2017).

privacy it warrants to its customers. In fact, T-Mobile has emphatically failed to do so for over a decade.

b. Michael Piri's T-Mobile Account is Compromised as Part of the Ongoing SIM Swap Fraud.

13. When Michael Piri, Plaintiff's brother, discovered his account had been hacked, he contacted T-Mobile and discovered that unauthorized persons had been contacting T-Mobile for several days prior to the date of the hack in an attempt to access his personal identifying information.

14. Using Michael's basic identifying information, the hackers employed a popular hacking tactic known as "social engineering" to pose as Michael. After successfully executing the hack, the hackers secured access to Michael's T-Mobile account.

15. T-Mobile's release of account specific information to the hacker over the phone was in direct violation of their express warranty and policy to not do so.[11] Specifically, T-Mobile warrants that it "has a duty[] to protect the confidentiality of [a customer's] account information . . . and do everything possible to ensure that [a customer's] account information is not shared with others without [their] consent." *Id*. In doing everything possible to prevent unauthorized access to a customer's account and confidential information, T-Mobile has "implemented various policies and measures to ensure that [its] interactions are with [a customer] or those [the customer has] authorize[d] to interact with [T-Mobile] on [the customer's] behalf – and not with others pretending to be [the customer] or claiming a right to access [the customer's] information." *Id*. Despite these warranties and various policies, the hacker was able to employ basic social engineering tactics to successfully circumvent T-Mobile's security.

[11] *Privacy & Security Resources: Account Verification*, https://www.t-mobile.com/company/privacy-resources/account-security/account-verification.html (last visited Oct. 18, 2017)

16. Once Michael Piri's T-Mobile account was compromised, his T-Mobile phone number was fraudulently ported to another carrier, he was indefinitely locked out of his T-Mobile account, he completely lost control of his online accounts and services tied to his phone number and other personal identifying information stored on his T-Mobile account, and approximately $1,000.00 was stolen from him.

17. Because Michael Piri's T-Mobile account is connected to Plaintiff's through a family plan, Michael immediately called Plaintiff after speaking with T-Mobile. Michael warned Plaintiff that the hackers potentially had access to Plaintiff's account once they had secured Michael's personal identifying information.

c. Plaintiff calls T-Mobile in an Attempt to Prevent any Potential Hack of his Account.

18. Quick to understand the gravity of the situation, Plaintiff contacted T-Mobile and other entities, such as Chase Bank, in order to report the attempted fraudulent action. Thus began Plaintiff's arduous trek through identity theft that completely consumed his everyday life for several months.

19. On the same day, Plaintiff contacted his bank to alert them to the possible fraud. The day after reporting the problem to T-Mobile, Plaintiff received a call from T-Mobile's fraud department warning him about the breach and instructing him to change his pin and contacting the company requesting the port. Plaintiff followed all of T-Mobile's instructions to prevent fraud.

20. At approximately 9:30AM on May 9, 2017, before Plaintiff's account and information had been compromised, Plaintiff contacted T-Mobile's fraud department, requested a password change on his account, and warned T-Mobile about the potential attempt by the hackers to port his phone number. By 11:30AM on the same day, Plaintiff, along with Michael Piri, again

contacted T-Mobile's fraud department and attempted to retrieve Michael Piri's phone number in order to prevent any further breaches.

21. By 12:15PM, Plaintiff contacted T-Mobile's customer care department in order to change his password. T-Mobile's representative consistently reassured Plaintiff that a confirmation to change his password would be sent to him, but Plaintiff never received any such confirmation. At 1:00PM, Plaintiff yet again contacted T-Mobile's fraud department to confirm his password was secure on the account. T-Mobile's agent confidently assured him that it was.

22. While Plaintiff actively sought to protect his identity from theft, the hackers also continued to attack Plaintiff's digital identity on all fronts. Within less than 24 hours following notice of the fraudulent action from Michael Piri, Plaintiff's phone number and account information had been completely compromised. Despite contacting T-Mobile at least four times within that 24-hour period and having been reassured by multiple T-Mobile representatives that his information and account were secure, T-Mobile improperly provided Plaintiff's account and password information to an unauthorized user without Plaintiff's consent and in direct violation of Plaintiff's requests and T-Mobile's warranties. Within 48 hours, Plaintiff's business accounts and information had been compromised. Within 72 hours, Plaintiff's entire identity – both personal and business – was no longer in his possession.

d. Despite Numerous Assurances of Security by T-Mobile, Plaintiff's T-Mobile Phone Number is Ported and His Identity is Stolen as Part of an Ongoing, Months-Long SIM Swap Fraud Exploiting a T-Mobile Security Deficiency.

23. Despite T-Mobile's confirmation of the security of Plaintiff's account and Plaintiff's repeated warnings to T-Mobile of an impending hack, Plaintiff's T-Mobile number was ported and he lost signal at approximately 10:30AM on May 10, 2017. Five minutes later, Plaintiff's personal and work email accounts were compromised with 2 Factor Authorization

("2FA") resets through his T-Mobile phone number: (512) 769-3026. Reacting to the ongoing hack, Plaintiff attempted to change the passwords for his email accounts, banking account, Paypal account, and several other service accounts.

24. At 11:30AM on May 10, 2017, Plaintiff again contacted T-Mobile's fraud department in order to report that T-Mobile had ported his number despite prior warnings by him to T-Mobile to prevent such an occurrence. At 12:30PM, Plaintiff obtained and activated a new T-Mobile phone number: (512) 704-3259. At 12:45PM, the hackers hard data reset Plaintiff's phone and various personal and business accounts. Consequently, Plaintiff lost his 2FA applications and all of his personal and business data including, but not limited to, irreplaceable family photos and videos, work communications, work calendar, his password keychain(s), all of his banking applications, and all of his business applications and work product.

25. Upon information and belief, Plaintiff was the victim of an ongoing SIM Swap Hack scheme exploiting a grave deficiency in T-Mobile's security infrastructure. While T-Mobile quickly patched the deficiency within less than 24 hours of knowing about it, the hack was known and used by "a bunch of sim swapping [hackers] . . . for quite a while" before T-Mobile ever knew of the deficiency.[12] In fact, the hack was so well-known throughout the hacking community that video tutorials of how to successfully execute it were uploaded to YouTube. *Id*. Experts, including a former National Security Agency ("NSA") hacker, have asserted that the deficiency was "relatively easy to detect" and T-Mobile's failure to detect it earlier indicates it was "obviously asleep at the wheel with monitoring." *Id*.

[12] *There's 'No Excuse' for the T-Mobile Bug That Helped Hackers Steal Accounts,* https://motherboard.vice.com/en_us/article/7xkyyz/t-mobile-customer-data-bug-hackers-no-excuse (last visited Oct. 19, 2017)

26. After diligently checking which accounts and what information had been compromised, Plaintiff again contacted T-Mobile's fraud department at 3:00PM on May 10, 2017. Shortly thereafter, Plaintiff's wife, Courtney Piri, notified him that their Chase Bank account had been compromised. Using information obtained from Plaintiff's T-Mobile account, the hackers had attempted to withdraw approximately $45,000.00 from Plaintiff's bank account.

e. The Hackers Contact Plaintiff and Hold His Identity Hostage in Exchange for a Ransom. Plaintiff Refuses, and the Hack Escalates.

27. At approximately 12:30AM on May 11, 2017, the hackers contacted Plaintiff via email and demanded payment of 1 (one) bitcoin (BTC) in exchange for their ceasing the infiltration via the ported T-Mobile number. Plaintiff refused to pay the ransom.

28. After Plaintiff's refusal, the hackers regained full control of Plaintiff's email accounts (both personal and business) and Apple ID, remote wiped his iPhone (containing irreplaceable personal and business data), locked both of his Apple Macbook laptops containing all of his personal and business data (e.g., client projects, vital business documents, etc.), locked his remote access keys for work servers, accessed over 1,000 passwords belonging to his clients, and acquired countless items of personal and business information (e.g., business entities' Employee Identification Numbers, clients' Social Security Numbers, intellectual property for software designs, etc.).

29. During this time, T-Mobile continued to breach its warranties and duties to Plaintiff. Already three days into the hack, and fully aware of the hack's occurrence, T-Mobile failed to honor Plaintiff's requests to protect his identity in any manner possible – no matter how minimal. This included Plaintiff's request that his newly provided T-Mobile phone number not forward his information to the hackers already in possession of his compromised T-Mobile account. T-Mobile failed to honor this simple request, and, as a result of T-Mobile's negligent,

deceptive, and breaching conduct, the hackers had access to Plaintiff's new T-Mobile phone number: (512) 704-3259 and were able to stay several steps ahead of Plaintiff at all times.

f. Despite Its Consistent Failures to Protect Plaintiff, His Account, and His Personal Identifying Information, T-Mobile Attempts to Convince Plaintiff That Its Security Can Be Trusted and That His Account and Information Are Safe.

30. By 1:54PM on Thursday, May 11, 2017, Plaintiff once again contacted T-Mobile's fraud department to update T-Mobile on the escalating situation. At this point in the hack's occurrence, T-Mobile still had not made even a single, minimal effort to contact Plaintiff and notify him of any fraudulent or questionable activity on his account, nor of any developments regarding the hack.

31. T-Mobile's representative expressly acknowledged the breaches on T-Mobile's behalf. At 4:11PM on May 11, 2017, T-Mobile's fraud department representative connected Plaintiff with T-Mobile's customer service representative in charge of handling Plaintiff's case. Despite the three prior breaches of Plaintiff's account, all of which were expressly acknowledged by T-Mobile's fraud department representative preceding and following escalation of the hack, T-Mobile's customer service representative attempted to convince Plaintiff that T-Mobile could still successfully protect his phone number, account, and any and all personal identifying information.

32. Finally, at 10:30AM on Friday, May 12, 2017, T-Mobile's fraud department representative informed Plaintiff that his phone number had been transferred back to T-Mobile. By this point in time, Plaintiff's entire digital identity and personal and business information had already been completely compromised for nearly two full days. Plaintiff's T-Mobile phone number and account were no longer of value to the hackers because they had already accessed and acquired all of the information they desired.

g. T-Mobile's Breaches of its Terms of Conditions, as well as its Negligent and Deceptive Acts Facilitated the Hack and Have Caused Plaintiff Months-Long, Economic, Emotional, and Mental Damages.

33. By the time T-Mobile finally transferred back Plaintiff's phone number, Plaintiff had already incurred immense personal expenses and immeasurable mental and emotional agony while attempting to re-secure his identity. During this time Plaintiff was unable to continue to work, his timelines (often set by clients, not him) were forced to be pushed back indefinitely, and his professional reputation as a secure, dependable developer was severely damaged.

34. To date, T-Mobile has caused Plaintiff to suffer considerable personal and financial expense and agony. T-Mobile's conduct becomes more egregious when considering Plaintiff had consistently put T-Mobile on notice of the hack well before it began.

35. Moreover, given its history with such breaches in security and based on prior cited experts' opinions, T-Mobile itself was, or should have also been, on notice independent of Plaintiff's warnings. In fact, federal law required T-Mobile to not only have notified Michael Piri and Plaintiff of the hack's occurrence immediately upon its discovery, but to also mitigate its effects.[13] T-Mobile, however, failed to ever do so.

36. T-Mobile has also refused to work with Plaintiff to restore him to his pre-hack state of being, despite its representative's express acknowledgment of the hack and accountability for the hack.

V. CAUSES OF ACTION

Count I - BREACH OF CONTRACT

37. Plaintiff realleges and incorporates by reference Paragraphs 1-35 above, as if fully set forth herein.

[13] 16 C.F.R. § 681.1 (2013) "The Red Flags Rule"

38. Plaintiff entered into a contract with T-Mobile when purchasing products and services from T-Mobile.

39. In exchange for its product and services, T-Mobile required Plaintiff to consent to its Terms and Conditions

40. Within its Terms and Conditions, T-Mobile represented that it used, and would continue to use, industry-leading security practices to protect Plaintiff's private personal information. For example, T-Mobile explicitly states that it will only allow third party access to a consumer's account if the third party is established as an "Authorized User" beforehand.[14] Only the account holder and Authorized User can "[m]ake changes to [an] account" and access its information, amongst other privileges. *Id*. T-Mobile further alleged, and Plaintiff reasonably relied to his detriment upon, its commitment "to safeguarding the personal and account information of [its] customers" via "established physical, technical and administrative safeguards."[15]

41. On information and belief, T-Mobile has failed to provide the requisite "physical, technical and administrative safeguards" intended to protect Plaintiff's account and personal identifying information. *Id*.

42. On information and belief, T-Mobile actively employed insufficient security practices for the protection of Plaintiff's confidential information. T-Mobile, via its representatives, agents, and/or employees, further failed to utilize the "extensive privacy security training [given] to all T-Mobile employees." *Id*. Despite being notified of the account's breach by Plaintiff, T-Mobile took active and knowing steps to facilitate Plaintiff's account's security

[14] *T-Mobile Terms & Conditions*, https://www.t-mobile.com/Templates/Popup.aspx?PAsset=Ftr_Ftr_TermsAndConditions&print=true (last visited Oct. 6, 2017)
[15] *About T-Mobile: Privacy and Security Resources*, https://www.t-mobile.com/company/privacy-resources/identity-theft.html (last visited Oct. 6, 2017)

breach. Specific examples of steps taken in furtherance of its active and knowing facilitation of the hack are set forth above in Paragraphs 6-13, which are incorporated by reference.

43. On information and belief, T-Mobile knows or should know that such activities facilitated Plaintiff's account's breach in security, including for example, allowing the continuance of the breach in spite of Plaintiff's numerous warnings otherwise.

44. By its actions, T-Mobile has injured Plaintiff and is liable to Plaintiff for breach of contract to the full extent permissible under law.

Count II – NEGLIGENCE

45. Plaintiff realleges and incorporates by reference Paragraphs 1-43 above, as if fully set forth herein.

46. T-Mobile owed a duty to Plaintiff to utilize security practices that would protect his confidential, private personal information provided to T-Mobile against the very sort of attack that gives rise to this suit. *See generally* Footnote 3.

47. T-Mobile breached the aforementioned duty when it failed to properly use minimum-security practices that would protect the confidential, private personal information of Plaintiff. May it be reiterated that T-Mobile failed to do so, and subsequently breached, even after being explicitly put on notice by Plaintiff several times prior to escalation of the hack of Plaintiff's T-Mobile account. *See* Paragraphs 6-13 above.

48. As a direct and proximate cause of T-Mobile's failure to use the appropriate security practices to protect Plaintiff's confidential, private personal information, Plaintiff's account was hacked causing Plaintiff's information to be accessed by, and disseminated to, unauthorized individuals.

49. The breach of Plaintiff's T-Mobile account caused direct and substantial damages to Plaintiff, as well as the unfortunate and likely possibility of future harm through the

dissemination of Plaintiff's confidential, private personal information related to both his business and personal lives. Moreover, the unfortunate possibility of yet another identity theft hack against Plaintiff is also an increasingly likely reality now that his business and personal confidential, private information has already been compromised and disseminated as a result of T-Mobile's breach.

50. The law also imposes an affirmative duty on T-Mobile, as Defendant, to timely disclose the theft of Plaintiff's confidential, personal private information so that Plaintiff could be vigilant in attempting to determine if any of his other accounts or assets had been compromised via the theft. Tex. Bus. & Com. Code § 521.053.

51. Through T-Mobile's failure to provide timely and clear notification of the aforesaid breach, T-Mobile negligently prevented Plaintiff from taking meaningful, proactive steps to investigate, and mitigate, possible identity theft and other related harms. Instead, Plaintiff was made aware of the breach himself *after* it had occurred and escalated as a result of the negligent acts or omissions of T-Mobile.

52. In engaging in the forgoing negligent acts and omissions, T-Mobile committed the common law tort of negligence. For the reasons stated above, T-Mobile's conduct was negligent and departed from the reasonable standards of care including, but not limited to the following:

- Failing to adequately protect Plaintiff's confidential, private personal information; and
- Failing to provide Plaintiff with a timely and sufficient notice of the theft of his confidential, private personal information.

53. Plaintiff did not contribute to the breach or subsequent and related misuse of his confidential, private personal information as described in this Complaint.

54. As a direct and proximate result of T-Mobile's actions and inactions, Plaintiff has suffered damages and been put at risk of future identity theft. T-Mobile is liable to Plaintiff for the reasonable harms directly suffered and costs of services, both present and future, required to mitigate such harms sustained as a result of Plaintiff's identity theft.

Count III – NEGLIGENCE PER SE

55. Plaintiff realleges and incorporates by reference Paragraphs 1-53 above, as if fully set forth herein.

56. Section 5 of the FTC Act prohibits the "unfair . . . practice in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as T-Mobile, of failing to utilize reasonable measures to protect the confidential, private personal information of consumers.

57. T-Mobile violated Section 5 of the FTC Act by failing to use reasonable and requisite measures to protect Plaintiff's confidential, private personal information. T-Mobile further violated Section 5 of the FTC Act by failing to comply with applicable and requisite industry standards regarding the protection of consumers' private identifying information. T-Mobile's conduct in this matter was particularly unreasonable given the nature and amount of Plaintiff's information that was obtained, Plaintiff's numerous express notices to T-Mobile of the ongoing breach of his data, and the foreseeable consequences of the breach's occurrence given T-Mobile's numerous sufferings of hacks of a similar nature to Plaintiff's over the course of several years, including, specifically, the immense damages that would result to Plaintiff related to the breach of his data in this manner.

58. T-Mobile's violation of Section 5 of the FTC Act constitutes negligence per se.

59. T-Mobile also violated Section 1681 of the Fair Credit Reporting Act (FCRA) and Section 521 of the Texas Business & Commerce Code (TBOC), respectively. Each of these violations, too, constitute negligence per se.

60. Plaintiff is within the class of persons that the FTC Act, the FCRA, and the TBOC were intended to protect.

61. The harm that occurred as a result of the breach of Plaintiff's confidential, private personal information is precisely the type of harm that the FTC Act, the FCRA, and the TBOC, by way of tie-in via the Texas Deceptive Trade Practices Act (DTPA), were intended to guard against. For example, the FTC has previously pursued enforcement actions against businesses that have caused harms to consumers of a similar nature to those stated within this complaint. Those harms, which are again similar to the harms Plaintiff suffered and continues to suffer from in this matter, were the direct result of the business' failure(s) to utilize reasonable security measures and avoid unfair and deceptive practices.

62. Upon information and belief, T-Mobile engaged in this misconduct recklessly, in conscious neglect of duty and in callous indifference as to the consequences of its misconduct, and, in the alternative, with such want of care as would raise a presumption of a conscious indifference to the consequences suffered. For example, T-Mobile did not at any point exercise the bear minimum security measures to protect Plaintiff's information despite being notified of the ongoing hack by Plaintiff himself, T-Mobile did not warn Plaintiff himself of the hack's occurrence in a timely manner or any manner whatsoever, and T-Mobile, via its agents, employees, and representatives, consistently failed to enforce the very security measures it warrants to its consumers it extensively trains all of its employees in and that are required by the Red Flags Rule.[16]

[16] *See* n. 13, *supra*.

63. T-Mobile – by way of Plaintiff's own express notices to it, alleged extensive security training and measures, and the numerous previous hacks of a similar nature suffered by its customers over the course of several years – was or should reasonably have been aware of its misconduct and of the foreseeable injury that would probably result, and with reckless indifference to consequences, consciously and intentionally committed the wrongful acts and omissions herein. T-Mobile's actions and omissions were, therefore, not just negligent, but grossly negligent, reckless, willful, and wanton.

64. As a direct and proximate result of T-Mobile's negligence *per se*, Plaintiff suffered and will continue to suffer injury, which includes, but is not limited to:

- Monetary damages, as alleged above;
- Inconvenience and exposure to a heightened, imminent risk of fraud, identity theft, and financial harm to Plaintiff's business and person;
- Continued incurrence on an indefinite basis of out-of-pocket costs for obtaining, and rectifying, credit reports, credit freezes, credit monitoring services, and other protective measures to deter or detect identity theft and its consequences for Plaintiff's business and person; and
- The diminished value of Plaintiff's confidential, private personal and business information due to the unauthorized acquisition of such information facilitated by T-Mobile.

Through its failure to timely discover and provide clear notification of the hack against Plaintiff's account, T-Mobile prevented Plaintiff from taking meaningful, proactive steps to secure and/or mitigate damages to his business and personal confidential, private information.

65. But for T-Mobile's violation of the applicable laws and regulations set forth above, Plaintiff's confidential, private information would not have been accessed by unauthorized individuals.

66. The damages to Plaintiff were a direct, proximate, and reasonably foreseeable result of T-Mobile's breaches of the applicable laws and regulations set forth above.

67. Therefore, Plaintiff is entitled damages in an amount to be proven at trial.

Count IV – VIOLATION OF THE TEXAS DECEPTIVE TRADE PRACTICES ACT

68. Plaintiff realleges and incorporates by reference Paragraphs 1-66 above, as if fully set forth herein.

69. Plaintiff is a "consumer" as that term is defined by the DTPA. Tex. Bus. Com. Code § 17.45. T-Mobile is a "person" engaged in "trade" or "commerce" as defined by the DTPA, and is therefore subject to Plaintiff's action under the DTPA for use or employment of violations of the "laundry list" or unconscionable actions. *Id*.

70. At all times relevant, the Texas Deceptive Trade Practices Act ("DTPA") prohibits the commission of "false, misleading, or deceptive acts or practices" in trade or commerce within the meaning of Tex. Bus. & Com. Code § 17.46(a). T-Mobile, by failing to initially prevent and later successfully facilitating the hack of Plaintiff's private account despite Plaintiff's numerous warnings of the hack's occurrence, knowingly committed "false, misleading, or deceptive acts or practices." Tex. Bus. Com. Code § 17.46(a).

71. Specifically, T-Mobile, via its fraud and customer service representatives Kay and Salvatore Ortega, respectively, consistently told and assured Plaintiff that it was able to protect his T-Mobile number and account information. Furthermore, T-Mobile, via its website and Terms of

Service, represents that it employs "considerable resources . . . dedicate[d] to customer security."[17] T-Mobile further represents that "[u]nless [it] can verify the caller's identity through [its various security] methods, [its] policy is not to release any account specific information over the phone."[18] Via its Privacy Policy, T-Mobile also represents that it uses "a variety of physical, electronic, and procedural safeguards to protect Personal Information from unauthorized access, use, or disclosure while it is under [T-Mobile's] control."[19] In compliance with federal law, T-Mobile also represents that it has a duty to notify customers of any changes to their password, back-up means of authentication, and online account.[20]

72. T-Mobile consistently failed to employ the aforementioned policies and safeguards it represents to. It also never notified Plaintiff of the hack or its escalation, even though federal law required it. In failing to do so, T-Mobile deceptively and falsely represented to Plaintiff that its services had security characteristics or benefits that they did not. Tex. Bus. Com. Code § 17.46(b)(5). The oral and written statements made to Plaintiff by T-Mobile also constitute T-Mobile's false, deceptive, and misleading representation to Plaintiff that its services were of a particular security standard, quality, or grade compliant with federal law when they were not. Tex. Bus. Com. Code § 17.46(b)(7). By not complying with its own Terms of Service, Privacy Policy, or representations and policies, T-Mobile also falsely and deceptively represented to Plaintiff that its agreements for service conferred or involved obligations of, and rights to, security and data protection which they did not have or involve. Tex. Bus. Com. Code § 17.46(b)(12).

---

[17] *Password Security: Security and Your Wireless Device*, https://www.t-mobile.com/company/privacy-resources/account-security/password-security.html (last visited Nov. 30, 2017)
[18] *Privacy & Security Resources: Account Verification*, https://www.t-mobile.com/company/privacy-resources/account-security/account-verification.html (last visited Oct. 18, 2017)
[19] *Privacy Policy*, https://www.t-mobile.com/company/website/privacypolicy.aspx#fullpolicy (last visited Nov. 30, 2017)
[20] *Customer Proprietary Network Information*, https://www.t-mobile.com/company/privacy-resources/cpni.html (last visited Nov. 30, 2017)

73. Furthermore, T-Mobile's failure to satisfy its express and implied warranties of security and protection made to Plaintiff constitute a false, deceptive, and misleading representation that their guarantees and warranties conferred or involved rights to security and privacy that they did not have or involve. Tex. Bus. Com. Code § 17.46(b)(20).

74. Specifically, T-Mobile, via its Device Protection Warranty, warranted that it would cover the complete "replacement of a device in the event of . . . theft, even after the manufacturer's warranty expires."[21] Because of T-Mobile's failure to prevent the hack's occurrence and escalation, Plaintiff's entire device was compromised and constructively stolen from his possession. Instead of T-Mobile replacing Plaintiff's device pursuant to its Device Protection Warranty, Plaintiff had to replace his device at his own expense of $1,000.00. This failure, among others previously mentioned regarding T-Mobile's Terms of Service, Privacy Policy, and representations, to comply with its own oral and written guarantees and warranties constitute breaches by T-Mobile of its express and implied warranties under Tex. Bus. Com. Code 17.50(a)(2).

75. Thus, under the protection afforded to Plaintiff by the DTPA, Plaintiff sought or acquired goods or services by lease or purchase from T-Mobile which forms the basis of the complaint against T-Mobile, as specified above.

76. Said conduct was a producing cause of damages to Plaintiff.

77. Plaintiff has suffered economic and mental anguish damages within the jurisdictional limits of this court.

78. The actions of T-Mobile have violated the DTPA in one or more of the following particulars:

[21] *Device Protection*, https://support.t-mobile.com/docs/DOC-1250 (last visited Nov. 30, 2017)

- Representing that the goods or services had characteristics which they did not have. Tex. Bus. Com. Code § 17.46(b)(5).
- Representing that the goods or services were of a particular standard, quality, or grade when they were of another. Tex. Bus. Com. Code § 17.46(b)(7)
- Representing that an agreement confers or involves rights, remedies, or obligations which it does not have or involved, or which are prohibited by law. Tex. Bus. Com. Code § 17.46(b)(12)
- Representing that a guaranty or warranty confers or involves rights or remedies which it does not have or involve. Tex. Bus. Com. Code § 17.46(b)(20).
- Breach of express and/or implied warranty. Tex. Bus. Com. Code § 17.50(a)(2)

79. Plaintiff is entitled to and hereby sues for pre-judgment interest as allowed by law.

80. Plaintiff is entitled to and hereby sues for reasonable attorney's fees, including attorney's fees predicated upon appeal.

81. Plaintiff has given a demand letter to T-Mobile, more than 60 days prior to prosecuting the DTPA claim to conclusion. T-Mobile, to date, has not responded to the letter, nor has it made any effort to resolve this matter prior to commencement of this lawsuit by Plaintiff.

82. Plaintiff has performed all conditions precedent or same have occurred, entitling Plaintiff to recover under its claims against T-Mobile.

83. Through its inaction and actual awareness of its security deficiencies, T-Mobile acted knowingly and intentionally by representing to Plaintiff that T-Mobile could protect his identity, and that it would take action to defend against identify theft. As a result, T-Mobile is liable for treble Damages under the DTPA. Tex. Bus. & Com. Code § 17.50(b)(1).

Count V – INVASION OF PRIVACY

84. Plaintiff realleges and incorporates by reference Paragraphs 1-83 above, as if fully set forth herein.

85. T-Mobile invaded or facilitated the invasion of Plaintiff's privacy by turning over Plaintiff's confidential, private personal information to an unauthorized third party without the effective consent of Plaintiff. In fact, Plaintiff repeatedly notified T-Mobile of his refusal to consent to the provision of the information to the third party hackers, and T-Mobile, via its agents, representatives, and/or employees, was explicitly aware of Plaintiff's request. Even still, T-Mobile directly provided access to Plaintiff's confidential, private personal information via its actions or omissions.

86. Upon information and belief, Plaintiff has been victimized by identity theft as a direct result of T-Mobile's decision to release Plaintiff's confidential, private personal information to the unauthorized third party. T-Mobile allowed Plaintiff's privacy to be open to unauthorized individuals who could, and did, use the information to the detriment of Plaintiff.

87. As proximate result of T-Mobile's actions in sharing Plaintiff's confidential information with unauthorized third parties, Plaintiff has suffered damages and seeks recovery to the full extent permissible within the jurisdictional limits of this Court for the invasion of Plaintiff's privacy that T-Mobile facilitated.

Count VI – RESPONDEAT SUPERIOR

88. Plaintiff realleges and incorporates by reference Paragraphs 1-86 above, as if fully set forth herein.

89. T-Mobile is vicariously liable for the acts and/or omissions of any and all of its agents, representatives, and/or employees utilized by T-Mobile with regard to the fraudulent action and identity theft that is the basis of this lawsuit.

VI. DEMAND FOR JURY TRIAL

90. Plaintiff demands a trial by jury on all issues, claims, and causes of action so triable.

VII. PRAYER FOR RELIEF

91. WHEREFORE, PREMISES CONSIDERED, Plaintiff, DAVID REZA PIRI, respectfully requests that Defendants, T-MOBILE US, INC. and T-MOBILE USA, INC., be cited to appear and answer herein, and that on final trial of this cause, that Plaintiff have and recover over and against the Defendants, jointly and severally, as follows:

A. T-Mobile explicitly breached its contract (i.e., Terms & Conditions) with Plaintiff;

B. T-Mobile acted negligently in the above stated matter;

C. T-Mobile's actions and/or omissions were negligent *per se*;

D. T-Mobile violated several provisions of the Texas Deceptive Trade Practices Act, including demonstrating evidence of unconscionability;

E. An order under Tex. Bus. & Com. Code § 521.102 & 521.103(a) that Plaintiff is, in fact, a victim of identity theft;

F. T-Mobile directly invaded the privacy of Plaintiff, or contributed to and/or facilitated Plaintiff's invasion of privacy;

G. T-Mobile is vicariously liable for the actions and/or omissions of any and all of its agents, representatives, and/or employees involved in this matter;

H. Actual damages;

I. Economic and mental anguish damages;

J. Treble damages under the DTPA;

K. Reasonable and necessary attorney's fees and costs;

L. Prejudgment and post judgment interest at the maximum rate allowable by law;

M. Costs associated with this lawsuit's commencement and continuance; and

N. Such other relief, including other monetary and equitable relief, as this Court deems just and proper.

Dated: February 14, 2018

Respectfully Submitted,

/s/ Austin F. Pennington
Austin F. Pennington
Texas State Bar No. 24081432
austin@pfdallas.com

THE PENNINGTON FIRM, P.C.
10300 N. Central Expy., Suite 500
Dallas, TX 75231
Telephone (214) 494-9916
Facsimile: (214) 720-2309

ATTORNEY FOR REZA PIRI

JS 44 (Rev. 07/16)

CIVIL COVER SHEET

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

I. (a) PLAINTIFFS

Reza Piri

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

(c) Attorneys *(Firm Name, Address, and Telephone Number)*
The Pennington Firm, P.C.
10300 N. Central Expy., Suite 500, Dallas, Texas 75231
214-494-9916

DEFENDANTS

T-Mobile US, Inc.
T-Mobile USA, Inc.
T-Mobile USA, Inc.

County of Residence of First Listed Defendant King County, Washington
(IN U.S. PLAINTIFF CASES ONLY)

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

Attorneys *(If Known)*

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

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

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

(For Diversity Cases Only)

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

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

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

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
- ☐ 840 Trademark

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

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

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

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

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

PRISONER PETITIONS

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

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

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

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

VI. CAUSE OF ACTION

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

Brief description of cause:
Breach of contract, negligence, invasion of privacy

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
03/29/2018

SIGNATURE OF ATTORNEY OF RECORD
Austin F. Pennington

FOR OFFICE USE ONLY

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

Print Save As... Reset

INSTRUCTIONS FOR ATTORNEYS COMPLETING CIVIL COVER SHEET FORM JS 44

Authority For Civil Cover Sheet

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

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

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

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

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

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

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

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

VI. **Cause of Action.** Report the civil statute directly related to the cause of action and give a brief description of the cause. **Do not cite jurisdictional statutes unless diversity.** Example: U.S. Civil Statute: 47 USC 553 Brief Description: Unauthorized reception of cable service

VII. **Requested in Complaint.** Class Action. Place an "X" in this box if you are filing a class action under Rule 23, F.R.Cv.P.
Demand. In this space enter the actual dollar amount being demanded or indicate other demand, such as a preliminary injunction.
Jury Demand. Check the appropriate box to indicate whether or not a jury is being demanded.

VIII. **Related Cases.** This section of the JS 44 is used to reference related pending cases, if any. If there are related pending cases, insert the docket numbers and the corresponding judge names for such cases.

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