IN THE UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF GEORGIA

ATLANTA DIVISION

JOHN L. CUNNIFF, on behalf of himself and all others similarly situated, Plaintiff, v. EQUIFAX, Inc., Defendant.	Civil Action No. **COMPLAINT – CLASS ACTION** **JURY TRIAL DEMANDED** 1:18-CV-1071

Plaintiff JOHN L. CUNNIFF ("Plaintiff"), on behalf of himself and all others similarly situated, alleges as follows:

INTRODUCTION

1. Plaintiff brings this action individually and on behalf of a Class of California citizens ("Class") whose personal information was stolen due to Equifax's failure to utilize adequate cybersecurity mechanisms to protect its customers' personal data. As a direct result, millions of California citizens' personal information has been compromised by Equifax. Equifax, one of the three major consumer credit reporting agencies in the United States, was hacked and the data of these consumers was stolen as a result of Equifax's conduct (the "Hack").

The Hack occurred during mid-May through July 2017 and Equifax discovered the Hack on July 29, 2017. However, Equifax waited more than a month from the end of the Hack — until September 7, 2017 — to advise the millions of affected users that their private, personal information had been stolen.

2. It was not until September 7, 2017 that Equifax first revealed that a website application vulnerability allowed hackers to breach past and current users' personal information, including names, Social Security numbers, birth dates, addresses, and, in some instances, driver's license numbers. In addition, credit card numbers for approximately 209,000 U.S. users, and certain dispute documents with personal identifying information for approximately 182,000 U.S. users, were accessed. Equifax concealed the data breach, while at least three executive officers profited from selling thousands of shares of Equifax stock in the days following discovery of the breach.

3. This Hack is, perhaps, the largest ever in the United States and is at least the third major cybersecurity incident for Equifax since 2015. Despite a large number of recent cyber-attacks and warnings that Equifax must take more pro-active steps to improve its cyber security and data breach mechanisms, Equifax failed to secure the personal information of its users. Among its many failures, Equifax failed to use proper security methodologies to prevent and detect

unauthorized breaches of its information security systems. Likewise, Equifax failed to implement standard internet technology safeguards.

4. As a direct result of Equifax's cybersecurity failures, Plaintiff and the Class of California citizens have been damaged.

JURISDICTION AND VENUE

5. This Court has jurisdiction under 28 U.S.C. § 1332(d) because: (a) this matter was brought as a class action under Fed. R. Civ. P. 23; (b) the class (as defined below) has more than 100 members; (c) the amount at issue exceeds $5,000,000, exclusive of interest and costs; and (d) at least one proposed Class member is a citizen of a state different from Equifax.

6. This Court has personal jurisdiction over Equifax because Equifax transacts substantial business in this judicial district.

7. Venue is proper in this Court under 28 U.S.C. § 1391 because, inter alia, Equifax regularly conducts substantial business in this district and is therefore subject to personal jurisdiction, Plaintiff resides in this district and because a substantial part of the events giving rise to the Complaint arose in this district.

8. This action is not subject to arbitration. Equifax states on its website: "NO WAIVER OF RIGHTS FOR THIS CYBERSECURITY INCIDENT – In response to consumer inquiries, we have made it clear that the arbitration clause and class action waiver included in the Equifax and TrustedID Premier terms of

use does not apply to this cybersecurity incident." (See https://www.equifaxsecurity2017.com/)

THE PARTIES

9. Plaintiff John L. Cunniff is a natural person, California citizen, and resident of Mountain View, California. Plaintiff Cunniff is one of the approximately 143 million Equifax users — including an estimated 17 million California citizens — whose personal information was compromised because Equifax did not take reasonable steps to secure such information.

10. Defendant Equifax is a Georgia incorporated company headquartered at 1550 Peach Street, N.W., Atlanta, Georgia. Equifax is a member of the S&P 500, and its common stock trades on the New York Stock Exchange under the symbol EFX.

FACTS

11. There are three major credit reporting agencies in the United States: Equifax, Experian, and TransUnion. These agencies are responsible for running the reports that are used to calculate consumers' credit scores; impacting their ability to get a mortgage, buy a car, or engage in any number of other financial transactions.

12. Equifax organizes and analyzes data on more than 820 million consumers and more than 91 million businesses worldwide. Its database includes

employee data contributed from more than 7,100 employers. Equifax operates or has investments in 24 countries spanning North America, Central and South America, Europe and the Asia Pacific region. Last year, Equifax made $3.1 billion in revenue.

13. The Equifax website describes identity theft as "when someone steals your personal information – such as your name, Social Security number, and date of birth – typically to hijack your credit and use it to open up new credit accounts, take out loans in your name, or access your bank or retirement accounts."

14. The Equifax data breach is one of the largest breaches ever. From mid-May through July 2017, "Criminals exploited a U.S. website application vulnerability to gain access to certain files" held by Equifax. These files contained the names, Social Security numbers, birth dates, and addresses and, in some instances, driver's license numbers of some 143 million U.S. consumers. In addition, the credit card numbers for approximately 209,000 U.S. consumers, and certain dispute documents with the personal identifying information for approximately 182,000 U.S. consumers were accessed.

15. The vulnerability identified by Equifax as the cause of this data breach had been discovered and patched some two months before the data breach. Equifax did not update its website applications to fix this issue, despite reports back in March that hackers were actively targeting this vulnerability. Equifax's

website indicates that patching of this vulnerability did not occur until late July, after the breach had occurred.

16. On July 29, 2017, Equifax's Security team observed suspicious network traffic associated with its U.S. online dispute portal web application. In response, the Security team investigated and blocked the suspicious traffic that was identified. The Security team continued to monitor network traffic and observed additional suspicious activity on July 30, 2017. In response, the company took offline the affected web application that day. The company's internal review of the incident continued. Upon discovering a vulnerability in the Apache Struts web application framework as the initial attack vector, Equifax patched the affected web application before bringing it back online.

17. "Apache Structs is free, open-source software used to create Java web applications." However, as noted by Boris Chen, vice president of engineering at tCell in an interview with USA Today: "A single vulnerability in a web component should not result in millions of highly sensitive records being exfiltrated. Security controls should have existed at many points along the way to stop such a catastrophic outcome."

18. Equifax discovered the data breach on July 29, 2017, but did not make this information public until September 7, 2017, some 40 days later, when Equifax issued a press release. While the public was kept in the dark about this massive

breach, certain Equifax executives were not. Three senior executives "sold $1.8 million worth of shares in the days after Equifax discovered the breach."

19. Equifax knew of should have known that its systems were at-risk of hacking attacks based on previous attacks and reports that its internal system had weaknesses. Equifax failed to improve its data security after two data breaches that occurred in the last year: one in which hackers took valuable W-2 tax and salary data from the Equifax website and, in another, hackers took W-2 tax data from an Equifax subsidiary called TALX. Cybersecurity professionals interviewed by the *New York Times* concluded that there should have been more controls in place to prevent the most recent data breach, especially in light of these prior incidents.

20. The first Equifax security breach, which led to a class action lawsuit, stemmed from a May 2016 incident in which Equifax's W-2 Express website was breached, leading to the leak of 430,000 names, addresses, social security numbers, and other information. Equifax had clients' employees access their data with default PIN numbers made up of the last four digits of their social security number and four digit year of birth; assigned PIN numbers that were exceedingly easy for criminals to find on the internet. Equifax agreed to fix the underlying issue that led to this data breach, although it is unclear if the vulnerability has yet to be adequately addressed. The second prior Equifax data breach involving TALX was especially alarming because Equifax failed to discover that breach for almost a

year—from April 17, 2016 through March 29, 2017. This breach was not publicly disclosed until May 2017. That security breach related to hackers using personal information to guess client customer questions and ultimately reset their 4-digit PIN to gain access to customers' tax data.

21. Equifax also suffered smaller data breaches in January 2017, concerning LifeLock customer credit information, and a 2013-2014 breach of credit reports using personal information. In 2016, a vulnerability to cross-site scripting was discovered. Cross-site scripting, also known as XSS, is a process by which an attacker could send a link they create to users who would click on the link and long on to the website, revealing their user names and passwords and jeopardizing their personal information.

22. Security experts Kenneth White and Kevin Beaumont found that Equifax may have been susceptible to attacks because it uses old and discontinued technologies, like Netscape, IBM Websphere, Apache Struts, and Java. The vulnerabilities of those programs should have been addressed sooner given the sensitivity of information and the risk. AlienVault security advocate, Javvad Malik notes that "[c]ompanies like Equifax should know very well that data is the lifeblood of the organization and its crown jewels."

23. There are several governmental investigations already underway. The FTC has confirmed that it is investigating the Equifax data breach. The Consumer

Financial Protection Bureau is also investigating Equifax. The chairmen of the House Committee on Science, Space, and Technology and the House Committee on Oversight and Government Reform have said that their respective committees will investigate the Equifax data breach and have requested that Equifax produce documents to the Committees.

24. The FTC website suggests that people consider freezing their credit reports in light of this data breach, but this can be inconvenient in that it keeps consumers from opening new accounts unless they unfreeze them days in advance. Further, even if consumers freeze their credit reports with Equifax, they must also freeze them for Experian and TransUnion as well to give them the best protection. To add cost to this inconvenience of freezing credit reports, in some states these companies require consumers to pay a fee to freeze and unfreeze their credit reports. Unfortunately, even if consumers freeze their credit reports, they are not protected from potential fraudulent tax returns being filed with their information or people attempting to use their credit cards.

25. One security analyst was quoted in a *USA Today* article as saying that instead of checking credit card statements monthly, people need to now check them weekly and be hyper-vigilant if their information has been jeopardized.

26. In addition to common fears relating to identity theft like credit card use, people opening accounts in another person's name, and harm to a credit score,

consequences like medical identity theft (fake IDs used to pay for procedures and surgeries), tax fraud (filing false tax returns to profit from refunds), and synthetic identity theft (combining information from multiple victims to create a new identity) are also possible because of the depth of information stolen.

CLASS ACTION ALLEGATIONS

27. Pursuant to Federal Rules of Civil Procedure 23(a), (b)(2) and (b)(3), Plaintiff brings this action individually and on behalf of a class defined as follows:

> All California citizens whose personal information was compromised by the Hack disclosed by Equifax on September 7, 2017.

28. Plaintiff is a member of the proposed Class of California citizens he seeks to represent.

29. This action is brought and may properly be maintained as a class action pursuant to 28 U.S.C. § 1332(d). This action satisfies the procedural requirements set forth in FED. R. CIV. P. 23.

30. Plaintiff's claims are typical of the claims of the Class Members. Plaintiff and all Class Members were damaged by the same wrongful practices of Defendant.

31. Plaintiff will fairly and adequately protect and represent the interests of the Class of California citizens. The interests of Plaintiff are coincident with, and not antagonistic to, those of the Class of California citizens.

32. Plaintiff has retained counsel competent and experienced in complex class action litigation.

33. Members of the Class of California citizens are so numerous that joinder is impracticable. Plaintiff believes that there are millions of California citizens in the Class.

34. Questions of law and fact common to the members of the Class predominate over questions that may affect only individual Class Members, because Defendant has acted on grounds generally applicable to the entire Class. Thus, determining damages with respect to the Class of California citizens as a whole is appropriate.

35. There are substantial questions of law and fact common to the Class consisting of California citizens. The questions include, but are not limited to, the following:

a. Whether Defendant failed to employ reasonable and industry-standard measures to secure and safeguard its users' personal information;

b. Whether Defendant properly implemented and maintained security measures to protect its users' personal information;

c. Whether Defendant's cybersecurity failures harmed the personal information of California citizens whose information was accessed by

criminals or third parties who sought to gain financially from its improper use;

d. Whether Defendant negligently failed to properly secure and protect the personal information of California citizens;

e. Whether Plaintiff and other members of the Class of California citizens are entitled to injunctive relief; and

f. Whether Plaintiff and other members of the Class of California citizens are entitled to damages and the measure of such damages.

36. Class action treatment is a superior method for the fair and efficient adjudication of the controversy. Such treatment will permit a large number of similarly situated individuals to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, or expense that numerous individual actions would engender. Plaintiff knows of no special difficulty maintaining this action that would preclude its maintenance as a class action on behalf of California citizens.

COUNT ONE

NEGLIGENCE

(Plaintiff individually and All Class Members)

37. Plaintiff incorporates by reference each of the preceding paragraphs as if fully set forth herein.

38. Equifax had an affirmative duty to exercise reasonable care in protecting the personal information of its users. By maintaining their personal information in a database that was accessible through the Internet, Equifax owed Plaintiff and Class Members a duty of care to employ reasonable Internet security measures to protect this information.

39. Equifax, with reckless disregard for the safety and security of users' personal information it was entrusted with, breached the duty of care owed to Plaintiff and the Class by failing to implement reasonable security measures to protect its users' sensitive personal information. In failing to employ these basic and well-known Internet security measures, Equifax departed from the reasonable standard of care and violated its duty to protect the personal information of Plaintiff and all Class Members. Equifax further breached its duty of care by allowing the breach to continue undetected and unimpeded for a period of time after the hackers first gained access to Defendant's systems.

40. The unauthorized access to the personal information of Plaintiff and all Class Members was reasonably foreseeable to Equifax.

41. Neither Plaintiff nor other Class Members contributed to the security breach or Equifax's employment of insufficient and below-industry security measures to safeguard personal information.

42. It was foreseeable that Equifax's failure to exercise reasonable care in protecting personal information of its users would result in Plaintiff and the other Class Members suffering damages related to the loss of their personal information.

43. As a direct and proximate result of Equifax's reckless conduct, Plaintiff and Class Members were damaged. Plaintiff and Class members suffered injury through the public disclosure of their personal information, the unauthorized access to accounts containing additional personal information, and through the heightened risk of unauthorized persons stealing additional personal information. Plaintiff and Class Members have also incurred the cost of taking measures to identify and safeguard accounts put at risk by disclosure of the personal information stolen from Equifax.

COUNT TWO

VIOLATION OF CALIFORNIA CIVIL CODE § 1798.80, ET SEQ.

(Plaintiff individually and All Class Members)

44. Plaintiff incorporates by reference each of the preceding paragraphs as if fully set forth herein.

45. California Civil Code § 1798.80 et seq. (the "Customer Records Act") requires any person conducting business in California and owning computerized data to disclose data breaches to affected users if the breach exposed unencrypted personal information.

46. The Customer Records Act also requires that the notice be made in the most expedient time possible without any unreasonable delay.

47. Equifax failed to notify users of the Hack in an expedient fashion.

48. The Hack qualifies as a "breach of security system" of Equifax within the meaning of Civil Code § 1798.82(g).

49. Equifax is liable to Plaintiff and the Class Members for $500.00 pursuant to Civil Code § 1798.84(c), or up to $3,000.00 per class member if Equifax's actions are deemed willful, intentional, and/or reckless.

50. Equifax is also liable for Plaintiff's reasonable attorneys' fees and costs pursuant to Civil Code § 1798.84(g).

COUNT THREE

VIOLATION OF CALIFORNIA BUSINESS AND

PROFESSIONS CODE § 17200 ET SEQ.

(Plaintiff individually and All Class Members)

51. Plaintiff incorporates by reference each of the preceding paragraphs as if fully set forth herein.

52. California's Unfair Competition Law ("UCL") is designed to protect consumers from illegal, fraudulent, and unfair business practices.

53. Equifax's practice of representing that it adequately protected users' financial and personal information, while Equifax, in fact, employed insufficient

and ineffective security measures in order to cut costs, is a deceptive business practice within the meaning of the UCL. In fact, Equifax continues to employ insufficient security measures as to the non-public, financial and personal information of users. Thus, Equifax continues to engage in deceptive business practices.

54. Equifax's practice of withholding information about the Hack from its users is also a deceptive business practice within the meaning of the UCL, because users reasonably expect to be notified if their non-public, financial and personal information is compromised.

55. Equifax's practices are unfair because they allowed Equifax to profit while simultaneously exposing Equifax users, such as Plaintiff, to harm in the form of an increased risk of having their personal information stolen, which in fact occurred. Such harm was not foreseeable to Equifax's users, who expected Equifax to employ industry-standard security measures, including cybersecurity firewalls, to prevent a hack and investigative tools to timely discover one, and to promptly disclose any data breach.

56. Equifax's deceptive business practices induced Plaintiff and the Class to use Equifax's services and provide personal information to Equifax.

57. As a direct result of Equifax's deceptive business practices, Plaintiff and the Class have been and are being damaged.

COUNT FOUR

UNJUST ENRICHMENT

(Plaintiff individually and All Class Members)

58. Plaintiff incorporates by reference each of the preceding paragraphs as if fully set forth herein.

59. As a result of Equifax's misleading representations and omissions concerning the adequacy of its data security practices, Plaintiff and Class Members were induced to provide Equifax with their non-public, financial and personal information.

60. Equifax derived substantial revenues due to Plaintiff and the Class Members using Equifax's services, which maintained their non-public, financial and personal information, including through the sale of advertising directed at Plaintiff and the Class Members.

61. In addition, Equifax saved on the substantial cost of providing adequate data security to Plaintiff and the Class. Equifax's cost savings came at the direct expense of the privacy and confidentiality of the non-public, financial and personal information belonging to Plaintiff and the Class Members.

62. Plaintiff and the Class have been damaged and continue to be damaged by Equifax's actions, and Equifax has been unjustly enriched thereby.

63. Plaintiff and the Class are therefore entitled to damages as a result of Equifax's unjust enrichment, including the disgorgement of all revenue received and costs saved by Equifax as a result of the Hack.

WHEREFORE, Plaintiff and the Class pray for relief as set forth below.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the Class of California citizens, respectfully requests that the Court:

A. Determine that this action may be maintained as a class action pursuant to Federal Rule of Civil Procedure 23(a), (b)(2) and (b)(3);

B. Direct that reasonable notice of this action, as provided by Federal Rule of Civil Procedure 23(c)(2), be given to the Class;

C. Appoint Plaintiff as Class Representative;

D. Appoint Plaintiff's counsel as Class Counsel;

E. Enter judgment against Defendant and in favor of Plaintiff and the Class;

F. Adjudge and decree that the acts alleged herein by Plaintiff and the Class against Defendant constitute negligence, violation of California Civil Code § 1798.80, et seq., violation of California's Unfair Competition Law, and unjust enrichment;

G. Award all compensatory and statutory damages to Plaintiff and the Class in an amount to be determined at trial;

H. Award restitution, including the disgorgement of all revenue received and costs saved by Equifax as a result of the Hack, payable to Plaintiff and the Class;

I. Award punitive damages, including treble and/or exemplary damages, in an appropriate amount;

J. Enter an injunction permanently barring continuation of the conduct complained of herein, and mandating that Defendant and any successors in interest, be required to adopt and implement appropriate systems, controls, policies and procedures to protect the non-public, financial and personal information of Plaintiff and the Class;

K. Award Plaintiff and the Class the costs incurred in this action together with reasonable attorneys' fees and expenses, including any necessary expert fees as well as pre-judgment and post-judgment interest; and

//

//

//

//

L. Grant such other and further relief as is necessary to correct for the effects of Defendant's unlawful conduct and as the Court deems just and proper.

Dated: March 13, 2018

GROSS & BELSKY P.C.

By: _____
TERRY GROSS

Terry Gross (SBN 103878)
Adam C. Belsky (SBN 147800)
GROSS & BELSKY P.C.
201 Spear Street, Suite 1100
San Francisco, CA 94105
Telephone: (415) 544-0200
Facsimile: (415) 544-0201

1:18-CV-1071

JS 44 (Rev. 06/17)

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

John L. Cunniff, on behalf of himself and all other similarly situated

(b) County of Residence of First Listed Plaintiff Santa Clara, California
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys *(Firm Name, Address, and Telephone Number)*
Gross & Belsky P.C.
201 Spear Street, Suite 1100
San Francisco, California 94105

DEFENDANTS

Equifax, Inc.

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

Attorneys *(If Known)*

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

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

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

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

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

Click here for: Nature of Suit Code Descriptions.

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

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

TORTS

PERSONAL INJURY
- ☐ 310 Airplane
- ☐ 315 Airplane Product Liability
- ☐ 320 Assault, Libel & Slander
- ☐ 330 Federal Employers' Liability
- ☐ 340 Marine
- ☐ 345 Marine Product Liability
- ☐ 350 Motor Vehicle
- ☐ 355 Motor Vehicle Product Liability
- ☐ 360 Other Personal Injury
- ☐ 362 Personal Injury - Medical Malpractice

PERSONAL INJURY
- ☐ 365 Personal Injury - Product Liability
- ☐ 367 Health Care/ Pharmaceutical Personal Injury Product Liability
- ☐ 368 Asbestos Personal Injury Product Liability

PERSONAL PROPERTY
- ☒ 370 Other Fraud
- ☐ 371 Truth in Lending
- ☐ 380 Other Personal Property Damage
- ☐ 385 Property Damage Product Liability

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

PRISONER PETITIONS

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

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

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

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

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

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

PROPERTY RIGHTS
- ☐ 820 Copyrights
- ☐ 830 Patent
- ☐ 835 Patent - Abbreviated New Drug Application
- ☐ 840 Trademark

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

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

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

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

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

VI. CAUSE OF ACTION

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

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 Thomas W. Thrash, Jr. DOCKET NUMBER MDL-2800

DATE 03/13/2018 MDL 2800

SIGNATURE OF ATTORNEY OF RECORD T-A

FOR OFFICE USE ONLY

RECEIPT # AMOUNT APPLYING IFP JUDGE MAG. JUDGE

Class Action TWT 190 28:1332 fb