

PATRICIA M. BENWAY
1178 Annis Squam Harbour
Pasadena, MD 21122-2554,

*For herself and on behalf of all others
similarly situated,*

Plaintiffs,

v.

EQUIFAX INC.
c/o The Prentice Hall Corporation System, MA
7 St. Paul Street, Suite 820
Baltimore, MD 21202,

Defendant.

2017 OCT -5 AM 2:58

CIVIL DIVISION

IN THE
CIRCUIT COURT

FOR

BALTIMORE CITY, MARYLAND

Case No. _____

Jury Trial Demanded

CLASS ACTION COMPLAINT AND DEMAND FOR JURY TRIAL

Plaintiff, Patricia M. Benway ("Plaintiff" or the "Ms. Benway"), through her attorneys Gordon, Wolf & Carney, Chtd., for herself and on behalf of all others similarly situated, sues Defendant, Equifax Inc. ("Equifax"), and for their complaint state:

INTRODUCTION

1. Equifax is a global credit reporting agency that collects, stores, organizes, analyzes and disseminates data on hundreds of millions of consumers and tens of millions of business worldwide.

2. The data that Equifax collects includes Plaintiffs' and Class Members' personal identifying information ("PII") such as names, Social Security numbers, birth dates, addresses, driver's license numbers and credit card numbers.

3. Congress determined that fair and accurate credit reporting is essential to the banking system. Moreover, inaccurate credit reports lead to inefficiency, and unfair credit reports undermine public confidence, both of which harm the nation's banking system. Congress enacted

the Fair Credit Reporting Act, 15 U.S.C. § 1681 *et seq.* ("FCRA") as a balance between providing fair and accurate credit reporting in support of the nation's banking system, and protecting the privacy of consumers. To that end, the FCRA imposes duties on credit reporting agencies ("CRA"), such as Equifax, to protect consumers' PII.

4. One important attribute of the FCRA is the duty imposed on CRAs to safeguard the private information they collect on individuals from inappropriate disclosure. This duty, codified in 15 U.S.C. § 1681b, only allows a CRA to disclose a consumer's information for a "permissible purpose" as defined in the statute. To fulfill this duty, CRAs must maintain procedures to ensure that disclosures are only made for permissible purposes. 15 U.S.C. § 1681e(a).

5. The FCRA allows consumers to monitor access to their PII by giving them the right to request "All information in the consumer's file at the time of the request." 15 U.S.C. § 1681g(a)(1). Through such monitoring, a consumer can often determine if their identity has been stolen.

6. Consumers also may submit a fraud alert to a CRA for either a 90-day period or for an extended period of seven years. 15 U.S.C. § 1681c-1(a)-(b). After being notified of a fraud alert, the CRA must send notification to all CRAs that report information on a nationwide basis. 15 U.S.C. § 1681c-1(a)(1)(B). In the event a consumer requests an extended alert, the CRAs must remove the consumer from lists it sends to third parties in order to extend firm offers of credit, and keep the consumer off such lists for five years unless the consumer requests otherwise. 15 U.S.C. § 1681c-1(b)(1)(B).

7. Consumers also may independently monitor their credit information. Specifically, once a fraud alert notice has been given, the CRA must provide the consumer with the disclosures required under 15 U.S.C. § 1681g. When the consumer requests an extended fraud

alert, the consumer is entitled to two free disclosures under 15 U.S.C. § 1681g within the 12 months following the notification. 15 U.S.C. § 1681c-1(b).

8. These provisions of the FCRA set forth in paragraphs 1-5 (and others) allow consumers to determine if their identity has been stolen, and whether their efforts to protect such thefts have been successful. The FCRA facilitates consumers subject to potential fraud the ability to investigate and determine the extent of any suspected fraud they may have suffered.

9. Equifax failed to properly safeguard the PII of Plaintiff and the Class as required under 15 U.S.C. § 1681e(a), resulting in the May-July 2017 data breach.

10. Plaintiff, for herself and on behalf of all others similarly situated, brings this action to hold Equifax responsible for failing to protect and safeguard the Plaintiffs' and the Class Members' PII.

PARTIES, JURISDICTION & VENUE

11. Plaintiff Patricia M. Benway is a natural person and at all times pertinent to this action resided at 1178 Annis Squam Harbour, Pasadena, Maryland 21122-2554. At all times pertinent to this action, Plaintiff was a "consumer" as that term is understood under 15 U.S.C. § 1681a(c).

12. Defendant Equifax Inc. is a corporation incorporated under the laws of the State of Georgia with its principal place of business at 1550 Peachtree Street NE, Atlanta, Georgia. Equifax does substantial business in the State of Maryland through various subsidiaries, and each of these entities acts as agents of Equifax, or alternatively acts in concert with Equifax as alleged in this complaint. Equifax is a "consumer reporting agency" as that term is defined in 15 U.S.C. § 1681a(f).

13. This Court has subject-matter jurisdiction pursuant to § 1-501 of the Courts Article because the amount in controversy exceeds the jurisdictional amount of district court, and Plaintiffs seek a jury trial and to represent a class of persons who are similarly situated.

14. Equifax is subject to personal jurisdiction in this Court pursuant to § 6-103(b)(1-4) of the Courts Article.

15. Venue is appropriate in this Court pursuant to §6-201(a) of the Courts Article because Equifax's principal office in Maryland is in Baltimore City, and Equifax carries on a regular business in Baltimore City.

GENERAL ALLEGATIONS

16. On September 7, 2017, Equifax publicly acknowledged that it experienced a data breach in which an unknown third party (or parties) gained unauthorized access to its files containing the PII of Plaintiffs and the Members of the Class. Equifax acknowledged that the data breach started sometime in May 2017, and was discovered by Equifax on July 29, 2017. Equifax chose not to disclose the data breach to Plaintiffs, Members of the Class, or the public at large for nearly 6 weeks after it had been discovered.

17. On or around September 19, 2017, Equifax disclosed for the first time that in or about March 2017 it had suffered a similar data breach, but chose not to notify the Plaintiff, Members of the Class, or the public of this incident. Even with the knowledge of the vulnerability and defects in its cybersecurity system that resulted in the March data breach, Equifax did nothing to inform the Plaintiff, Members of the Class or the public of the significant risks and took no measures or inadequate measures to prevent the data breach that occurred in May-July 2017.

18. The 2017 incidents were not the only data breaches in Equifax's history. Equifax reported data breaches of one sort or another in 2013, 2014 and 2016, all as a result of either lax security, old technology, or both.

19. At all relevant times, Equifax was aware, or reasonably should have been aware, that the PII collected, maintained and stored in its computer systems is highly sensitive, susceptible to attack, and could be used by third parties for wrongful purposes, such as identity theft and fraud.

20. It is well known and the subject of numerous media reports that PII is highly coveted and a frequent target of hackers. Despite the frequent public announcements of data breaches of corporate entities, including Equifax competitor Experian, Equifax maintained an insufficient and inadequate system to protect the PII of Plaintiffs and Members of the Class.

21. PII is a valuable commodity. A "cyber black market" exists in which criminals openly post stolen payment card numbers, Social Security numbers, and other personal information on underground Internet websites. PII is as good as gold to identity thieves because they can use victims' personal data to open new financial accounts and take out loans in another person's name, incur charges on existing accounts, or clone ATM, debit or credit cards.

22. In the nearly six weeks between the discovery of the May-July 2017 data breach (July 29, 2017) and the public disclosure (September 7, 2017), Equifax made no effort to warn the Plaintiff, Members of the Class or the public of the risks to which they had been exposed. But three Equifax executives, during that six-week period, sold approximately \$1.8 million in Equifax stock: Chief Financial Officer John Gamble - \$946,000 on August 1, 2017; President of United States Information Solutions Joseph Loughran - \$584,000 on August 1, 2017; and President of Workforce Solutions Rodolfo Ploder - \$250,000 on August 2, 2017.

23. The May-July 2017 data breach was a direct and proximate result of Equifax's failure to properly safeguard and protect Plaintiff's and Members of the Class' PII from unauthorized access, use and disclosure, as required by the FCRA and industry practices, including failure to establish and implement appropriate administrative, technical and physical safeguards to ensure the security of Plaintiff's and Members of the Class' PII against reasonably foreseeable threats to the security or integrity of such information.

24. Equifax had the resources to prevent a breach, but willfully neglected to adequately invest in data security, despite its own experience with prior data breaches, and knowledge of the increasing number of well-publicized data breaches.

25. Had Equifax remedied the deficiencies in its data security systems, followed security guidelines, and adopted security measures as recommended by experts in the field, it could have prevented the May-July 2017 data breach and theft of Plaintiff's, and Members of the Class' PII.

CLASS ALLEGATIONS

26. Ms. Benway brings this claim on behalf of a Class that consists of:

All persons residing in the United States whose personally identifiable information (PII) was acquired by unauthorized persons in the May-July 2017 data breach.

Excluded from the Class are Equifax and any of its affiliates, parents or subsidiaries; all employees, officers and directors of Equifax; government entities, judges assigned to this case and their immediate families; and court staff.

27. The Class, as defined above, is identifiable. Equifax has access to information regarding the May-July 2017 data breach, the time period of the data breach, and which individual's PII was part of the May-July 2017 data breach. Ms. Benway is a member of the Class.

28. The Class is so numerous that joinder of all members is impracticable. Plaintiff does not know the exact number of members in the Class, but Equifax has publicly announced that the PII of at least 145.5 million individuals was compromised in the May-July 2017 data breach.

29. There are questions of law and fact which are not only common to the Class but which predominate over any questions affecting only individual Class members. The common and predominating questions include, but are not limited to:

- (a) Whether Equifax had a duty to protect PII;
- (b) Whether Equifax's security measures to protect their systems from a data breach were reasonable and adequate;
- (c) Whether Equifax failed to notify consumers of the data breach within a reasonable period of time;
- (d) Whether Ms. Benway and Class members are entitled to statutory damages;
- (e) Whether Ms. Benway and Class members are entitled to punitive damages; and
- (f) Whether Equifax knowingly or willfully maintained inadequate security measures to protect consumers' PII.

30. The claims of Ms. Benway are typical of the claims of the respective members of the Class within the meaning of Md. Rule 2-231(a)(3), and are based on and arise out of the same data breach, and the same actions and/or inactions of Equifax.

31. Ms. Benway will fairly and adequately protect the interests of the Class within the meaning of Md. Rule 2-231(a)(4). Ms. Benway is committed to vigorously litigating this matter to obtain relief for the Class, and has no conflicts of interest with the Class. Further, Ms. Benway has secured counsel experienced in handling consumer class actions and complex consumer litigation.

32. Neither Ms. Benway nor her counsel has any interests which might cause them not to vigorously pursue this claim.

33. The prosecution of separate actions by individual members of the Class would create a risk of establishing incompatible standards of conduct for Equifax within the meaning of Md. Rule 2-231(b)(1)(A).

34. Common questions of law and fact enumerated above predominate over questions affecting only individual members of the Class and a class action is the superior method for fair and efficient adjudication of the controversy within the meaning of Md. Rule 2-231(b)(3).

35. The likelihood that individual members of the Class will prosecute separate actions is remote due to the time and expense necessary to conduct such litigation.

36. Ms. Benway's counsel are experienced in class actions, and foresee little difficulty in the management of this case as a class action.

CAUSE OF ACTION

Willful Violation of the Fair Credit Reporting Act 15 U.S.C. §§ 1681 *et seq.*

37. Plaintiff restates and realleges the allegations contained in paragraphs 1 through 36 as if fully set forth herein.

38. Equifax violated the FCRA by providing impermissible access to Ms. Benway's and Class' consumer reports, and by failing to maintain adequate procedures to limit the furnishing of consumer reports to the purposes allowed under the FCRA.

39. Equifax acted willfully and recklessly because it knew or should have known about its legal obligations regarding data security, and that its data security measures were inadequate to satisfy its legal obligations. Equifax's willful conduct evidences evil motive, intent to injure, and ill will, constitutes actual malice.

40. Ms. Benway and the Class do not allege actual damages.

41. Ms. Benway and each member of the Class are entitled to recover statutory damages of not less than \$100 and not more than \$1,000.

42. Ms. Benway and the Class are entitled to punitive damages, costs of the action, and reasonable attorney's fees.

WHEREFORE, Patricia M. Benway, individually and on behalf of the Class, respectfully request that the Court enter judgment in their favor and against Equifax as follows:

- a. Certify the Class as defined herein pursuant to Md. Rule 2-231(b)(1) and (b)(3);
- b. Appoint Ms. Benway as Class Representative;
- c. Appoint Plaintiff's counsel as Class Counsel;
- d. Award statutory damages of not less than \$100 or more than \$1,000 to Ms. Benway and each member of the Class;
- e. Award punitive damages in an amount to be determined by the Court;
- f. Award the costs of litigation and reasonable attorney's fees; and
- g. Award such other relief that the Court deems just and proper.

[continued for signatures]

Respectfully submitted,



Richard S. Gordon

rgordon@GWCfirm.com

Martin E. Wolf

mwolf@GWCfirm.com

Benjamin H. Carney

bcarney@GWCfirm.com

GORDON, WOLF & CARNEY, CHTD.

100 W. Pennsylvania Ave., Suite 100

Towson, Maryland 21204

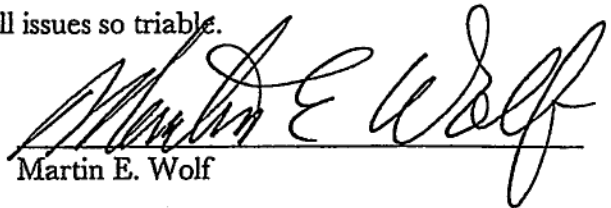
Tel. (410) 825-2300

Fax. (410) 825-0066

**Attorneys for Named Plaintiff and the
Putative Class**

JURY DEMAND

Plaintiff hereby demands a trial by jury of all issues so triable.



Martin E. Wolf

KING & SPALDING

King & Spalding LLP
1180 Peachtree Street N.E.
Atlanta, GA 30309-3521
Tel: +1 404 572 4600
Fax: +1 404 572 5100
www.kslaw.com

Phyllis B. Sumner
Direct Dial: +1 404 572 4799
Direct Fax: +1 404 572 5100
psumner@kslaw.com

September 7, 2017

To: Exhibit A; Distribution List

Re: Data Security Incident Affecting Equifax Inc.

Dear Sir or Madam,

I write on behalf of Equifax Inc. ("Equifax") regarding a cybersecurity incident potentially impacting information relating to approximately 143 million U.S. consumers. The approximate number of potentially impacted residents in your state is identified in Exhibit B. Equifax takes seriously its responsibility to protect the security of personal information, and our priority is to assist consumers who may have been impacted. The circumstances of the incident and the steps Equifax is taking to protect consumers are set forth below.

On July 29, 2017, Equifax discovered that criminals exploited a U.S. website application vulnerability to gain access to certain files. Upon discovery, Equifax acted immediately to stop the intrusion. The company promptly engaged a leading, independent cybersecurity firm that has been conducting a comprehensive forensic review to determine the scope of the intrusion, including the specific data impacted. Equifax also reported the criminal access to law enforcement and continues to work with authorities. While the company's investigation is substantially complete, it remains ongoing and is expected to be completed in the coming weeks.

The information accessed primarily includes 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. consumers, and certain dispute documents with personal identifying information for approximately 182,000 U.S. consumers, were accessed. The company has found no evidence of unauthorized access on Equifax's core consumer or commercial credit reporting databases.

Equifax has established a dedicated website, www.equifaxsecurity2017.com, to notify consumers of the incident, help them understand if they were potentially impacted, and provide steps they can take to protect against the potential misuse of their information. In addition to the website, Equifax will send direct mail notices to consumers whose credit card numbers or dispute documents with personal identifying information were impacted.

September 7, 2017

Page 2

Equifax is also offering to all U.S. consumers complimentary credit file monitoring and identity theft protection for one year, even if a consumer is not impacted by this incident. The offering, called TrustedID Premier, includes 3-Bureau credit monitoring of Equifax, Experian and TransUnion credit reports; copies of Equifax credit reports; the ability to lock and unlock Equifax credit reports; identity theft insurance; and Internet scanning for Social Security numbers. Information on how to enroll for this offering is included on the dedicated website. Additionally, Equifax has established a dedicated call center, 866-447-7559, available from 7:00 a.m. to 1:00 a.m. Eastern time, seven days a week, to answer questions about the incident, assist consumers in signing up for the complimentary service, and provide information about how to further protect personal information.

Please do not hesitate to contact me if you have any questions regarding this notification.

Sincerely,

A handwritten signature in black ink, appearing to read 'Phyllis B. Sumner', with a long horizontal line extending to the right.

Phyllis B. Sumner

Enclosures

Exhibit A - Distribution List

<p>Steve Marshall Office of the Alabama Attorney General Office of the Attorney General P.O. Box 300152 Montgomery, AL 36130-0152</p>	<p>Jahna Lindemuth Alaska Attorney General Office 1031 West 4th Avenue, Suite 200 Anchorage, AK 99501 attorney.general@alaska.gov</p>
<p>Mark Brnovich Office of the Arizona Attorney General 1275 West Washington Street Phoenix, AZ 85007-2926 AGInfo@azag.gov</p>	<p>Leslie Rutledge Arkansas Attorney General Office 323 Center Street, Suite 200 Little Rock, AR 72201 oag@ArkansasAG.gov</p>
<p>Xavier Becerra Office of the California Attorney General California Department of Justice P.O. Box 944255 Sacramento, CA 94244-2550</p>	<p>Cynthia H. Coffman Office of the Colorado Attorney General Colorado Department of Law Ralph L. Carr Judicial Building 1300 Broadway, 10th Floor Denver, CO 80203</p>
<p>George Jepsen State of Connecticut Attorney General's Office 55 Elm Street Hartford, CT 06106 ag.breach@ct.gov</p>	<p>Karl A. Racine District of Columbia Attorney General 441 4th Street, NW Washington, DC 20001 dc.oag@dc.gov</p>
<p>Matt Denn Delaware Attorney General Delaware Department of Justice Carvel State Building 820 N. French St. Wilmington, DE 19801 attorney.general@state.de.us</p>	<p>Pam Bondi Office of the Attorney General of Florida State of Florida The Capitol PL-01 Tallahassee, FL 32399-1050</p>
<p>Chris Carr Office of the Georgia Attorney General 40 Capitol Square, SW Atlanta, GA 30334</p>	<p>Douglas Chin Department of the Attorney General of Hawaii 425 Queen Street Honolulu, HI 96813</p>

<p>Hawaii Office of Consumer Protection Leiopapa A Kamehameha Building aka State Office Tower 235 South Beretania Street Honolulu, Hawaii 96813 dcca@dcca.hawaii.gov</p>	<p>Lawrence Wasden State of Idaho Attorney General's Office 700 W Jefferson St., Suite 210 P.O. Box 83720 Boise, ID 83720-0010</p>
<p>Lisa Madigan Illinois Attorney General's Office 100 W. Randolph Street Chicago, IL 60601 databreach@atg.state.il.us</p>	<p>Curtis T. Hill, Jr. Indiana Attorney General's Office Indiana Government Center South 302 W. Washington St., 5th Floor Indianapolis, IN 46204 IDTheft@atg.in.gov</p>
<p>Tom Miller Office of the Attorney General of Iowa Hoover State Office Bldg. 1305 E. Walnut Street Des Moines, IA 50319 consumer@iowa.gov</p>	<p>Derek Schmidt Kansas Attorney General 120 S.W. 10th Ave., 2nd Floor Topeka, KS 66612-1597</p>
<p>Andy Beshear Office of the Kentucky Attorney General 700 Capitol Ave, Suite 118 Frankfort, KY 40601-3449</p>	<p>Jeff Landry Office of the Louisiana Attorney General P.O. Box 94005 Baton Rouge, LA 70804-4095 ConsumerInfo@ag.louisiana.gov</p>
<p>Janet T. Mills Office of the Maine Attorney General 6 State House Station Augusta, ME 04333 breach.security@maine.gov</p>	<p>Brian E. Frosh Office of the Maryland Attorney General 200 St. Paul Place Baltimore, MD 21202-2202 Idtheft@oag.state.md.us</p>
<p>Maura Healey Office of the Attorney General of Massachusetts One Ashburton Place Boston, MA 02108-1518 ago@state.ma.us</p>	<p>Bill Schuette Michigan Department of Attorney General 525 W. Ottawa St. P.O. Box 30212 Lansing, MI 48909 miag@michigan.gov</p>
<p>Lori Swanson Office of the Minnesota Attorney General 445 Minnesota Street, Suite 1400 St. Paul, MN 55101-2131 Attorney.General@ag.state.mn.us</p>	<p>Jim Hood Mississippi Attorney General's Office 550 High Street Jackson, MS 39201</p>

<p>Josh Hawley Missouri Attorney General's Office Supreme Court Building 207 W. High St. P.O. Box 899 Jefferson City, MO 65102 attorney.general@ago.mo.gov</p>	<p>Tim Fox Office of the Montana Attorney General Justice Building, Third Floor 215 North Sanders P.O. Box 201401 Helena, MT 59620-1401 contactdoj@mt.gov</p>
<p>Montana Office of Consumer Protection P. O. Box 200151 Helena, MT 59620-0151 contactocp@mt.gov</p>	<p>Doug Peterson Nebraska Attorney General's Office 2115 State Capitol P.O. Box 98920 Lincoln, NE 68509 ago.consumer@nebraska.gov</p>
<p>Adam Paul Laxalt Office of the Nevada Attorney General 100 North Carson Street Carson City, NV 89701 AgInfo@ag.nv.gov</p>	<p>Gordon J. MacDonald New Hampshire Department of Justice 33 Capitol Street Concord, NH 03301 attorneygeneral@doj.nh.gov</p>
<p>Christopher S. Porrino Office of the New Jersey Attorney General RJ Hughes Justice Complex 25 Market Street, Box 080 Trenton, NJ 08625-0080 databreach@cyber.nj.gov</p>	<p>Hector Balderas Office of the New Mexico Attorney General 408 Galisteo Street Villagra Building Santa Fe, NM 87501</p>
<p>Eric T. Schneiderman Office of the New York Attorney General The Capitol Albany, NY 12224-0341</p>	<p>Josh Stein North Carolina Attorney General's Office 9001 Mail Service Center Raleigh, NC 27699-9001</p>
<p>Wayne Stenehjem North Dakota Attorney General's Office 600 E. Boulevard Ave. Dept. 125 Bismarck, ND 58505 ndag@nd.gov</p>	<p>Mike DeWine Ohio Attorney General's Office 30 E. Broad Street, 14th Floor Columbus, OH 43215</p>
<p>Mike Hunter Oklahoma Office of the Attorney General 313 NE 21st Street Oklahoma City, OK 73105</p>	<p>Ellen F. Rosenblum Office of the Oregon Attorney General Oregon Department of Justice 1162 Court Street, NE Salem, OR 97301-4096</p>

<p>Josh Shapiro Pennsylvania Office of Attorney General 16th Floor, Strawberry Square Harrisburg, PA 17120</p>	<p>Puerto Rico Departamento de Asuntos del Consumidor Ave. José De Diego, Pda. 22 Centro Gubernamental Minillas Edificio Torre Norte, Piso 7 San Juan, PR 00940 servicio@daco.pr.gov</p>
<p>Peter F. Kilmartin Office of the Rhode Island Attorney General 150 South Main Street Providence, RI 02903</p>	<p>Alan Wilson Office of the South Carolina Attorney General P.O. Box 11549 Columbia, SC 29211</p>
<p>Consumer Protection Division of the Department of Consumer Affairs P.O. Box 5757 Columbia, SC 29250</p>	<p>Marty J. Jackley South Dakota Attorney General's Office 1302 East Highway 14, Suite 1 Pierre, SD 57501-8501 consumerhelp@state.sd.us</p>
<p>Herbert H. Slatery, III Office of the Tennessee Attorney General and Reporter P.O. Box 20207 Nashville, TN 37202-0207</p>	<p>Ken Paxton Office of the Texas Attorney General P.O. Box 12548 Austin, TX 78711-2548</p>
<p>Sean D. Reyes Utah Office of the Attorney General Utah State Capitol Complex 350 N. State St., Suite 230 Salt Lake City, UT 84114-2320 uag@agutah.gov</p>	<p>TJ Donovan Vermont Attorney General's Office 109 State Street Montpelier, VT 05609-1001 ago.cap@vermont.gov</p>
<p>Mark R. Herring Office of the Virginia Attorney General 202 North Ninth Street Richmond, VA 23219</p>	<p>Bob Ferguson Washington State Office of the Attorney General 1125 Washington St SE P.O. Box 40100 Olympia, WA 98504-0100 SecurityBreach@atg.wa.gov</p>

<p>Patrick Morrissey Office of the West Virginia Attorney General State Capitol Complex Bldg. 1, Room E-26 Charleston, WV 25305 consumer@wvago.gov</p>	<p>Brad Schimel Office of the Wisconsin Attorney General Wisconsin Department of Justice P.O. Box 7857 Madison, WI 53707-7857</p>
<p>Peter K. Michael Wyoming Attorney General's Office Kendrick Building 2320 Capitol Avenue Cheyenne, WY 82002 ag.consumer@wyo.gov</p>	

Exhibit B – Approximate Number of Potentially Impacted Residents

Maryland – Approximately 2,964,180

KING & SPALDING

King & Spalding LLP
1180 Peachtree Street N.E.
Atlanta, GA 30309-3521
Tel: +1 404 572 4600
Fax: +1 404 572 5100
www.kslaw.com

Phyllis B. Sumner
Direct Dial: +1 404 572 4799
Direct Fax: +1 404 572 5100
psumner@kslaw.com

October 12, 2017

To: Exhibit A; Distribution List

Re: Data Security Incident Announced on September 7, 2017 Affecting Equifax Inc.

Dear Sir or Madam,

I write on behalf of Equifax Inc. ("Equifax") to follow up on the September 7, 2017 notification regarding a cybersecurity incident impacting the personal information of U.S. consumers. On October 2, 2017, Equifax announced that the cybersecurity firm Mandiant completed the forensic portion of its investigation of the cybersecurity incident announced on September 7, 2017 to finalize the consumers potentially impacted. The completed review determined that approximately 2.5 million additional U.S. consumers were potentially impacted, for a total of approximately 145.5 million. An updated approximate number of potentially impacted residents in your state is identified in Exhibit B.

Mandiant did not identify any evidence of additional or new attacker activity or any access to new databases or tables. Instead, this additional population of consumers was confirmed during Mandiant's completion of the remaining investigative tasks and quality assurance procedures built into the investigative process. To be clear, additional U.S. consumers identified, and the unauthorized access of information, all relate to the cybersecurity incident disclosed on September 7, 2017. To minimize confusion, Equifax will mail written notices to all of the additional potentially impacted U.S. consumers identified since the September 7 announcement. An unaddressed copy of that letter is attached as Exhibit C. The feature on the dedicated website, www.equifaxsecurity2017.com, that U.S. consumers may use to determine whether they may have been impacted has been updated to reflect the additional 2.5 million impacted U.S. consumers. Equifax takes seriously its responsibility to protect the security of personal information, and our priority is to assist consumers who may have been impacted.

Please do not hesitate to contact me if you have any questions regarding this update.

Sincerely,



Phyllis B. Sumner

CC: Zachary Fardon
Christopher C. Burris

Enclosures

Exhibit A - Distribution List

<p>Steve Marshall Office of the Alabama Attorney General Office of the Attorney General P.O. Box 300152 Montgomery, AL 36130-0152</p>	<p>Jahna Lindemuth Alaska Attorney General Office 1031 West 4th Avenue, Suite 200 Anchorage, AK 99501 attorney.general@alaska.gov</p>
<p>Mark Brnovich Office of the Arizona Attorney General 1275 West Washington Street Phoenix, AZ 85007-2926 AGInfo@azag.gov</p>	<p>Leslie Rutledge Arkansas Attorney General Office 323 Center Street, Suite 200 Little Rock, AR 72201 oag@ArkansasAG.gov</p>
<p>Xavier Becerra Office of the California Attorney General California Department of Justice P.O. Box 944255 Sacramento, CA 94244-2550</p>	<p>Cynthia H. Coffman Office of the Colorado Attorney General Colorado Department of Law Ralph L. Carr Judicial Building 1300 Broadway, 10th Floor Denver, CO 80203</p>
<p>George Jepsen State of Connecticut Attorney General's Office 55 Elm Street Hartford, CT 06106 ag.breach@ct.gov</p>	<p>Karl A. Racine District of Columbia Attorney General 441 4th Street, NW Washington, DC 20001 dc.oag@dc.gov</p>
<p>Matt Denn Delaware Attorney General Delaware Department of Justice Carvel State Building 820 N. French St. Wilmington, DE 19801 attorney.general@state.de.us</p>	<p>Pam Bondi Office of the Attorney General of Florida State of Florida The Capitol PL-01 Tallahassee, FL 32399-1050</p>
<p>Chris Carr Office of the Georgia Attorney General 40 Capitol Square, SW Atlanta, GA 30334</p>	<p>Douglas Chin Department of the Attorney General of Hawaii 425 Queen Street Honolulu, HI 96813</p>

<p>Hawaii Office of Consumer Protection Leiopapa A Kamehameha Building aka State Office Tower 235 South Beretania Street Honolulu, Hawaii 96813 dcca@dcca.hawaii.gov</p>	<p>Lawrence Wasden State of Idaho Attorney General's Office 700 W Jefferson St., Suite 210 P.O. Box 83720 Boise, ID 83720-0010</p>
<p>Lisa Madigan Illinois Attorney General's Office 100 W. Randolph Street Chicago, IL 60601 databreach@atg.state.il.us</p>	<p>Curtis T. Hill, Jr. Indiana Attorney General's Office Indiana Government Center South 302 W. Washington St., 5th Floor Indianapolis, IN 46204 IDTheft@atg.in.gov</p>
<p>Tom Miller Office of the Attorney General of Iowa Hoover State Office Bldg. 1305 E. Walnut Street Des Moines, IA 50319 consumer@iowa.gov</p>	<p>Derek Schmidt Kansas Attorney General 120 S.W. 10th Ave., 2nd Floor Topeka, KS 66612-1597</p>
<p>Andy Beshear Office of the Kentucky Attorney General 700 Capitol Ave, Suite 118 Frankfort, KY 40601-3449</p>	<p>Jeff Landry Office of the Louisiana Attorney General P.O. Box 94005 Baton Rouge, LA 70804-4095 ConsumerInfo@ag.louisiana.gov</p>
<p>Janet T. Mills Office of the Maine Attorney General 6 State House Station Augusta, ME 04333 breach.security@maine.gov</p>	<p>Brian E. Frosh Office of the Maryland Attorney General 200 St. Paul Place Baltimore, MD 21202-2202 Idtheft@oag.state.md.us</p>
<p>Maura Healey Office of the Attorney General of Massachusetts One Ashburton Place Boston, MA 02108-1518 ago@state.ma.us</p>	<p>Bill Schuette Michigan Department of Attorney General 525 W. Ottawa St. P.O. Box 30212 Lansing, MI 48909 miag@michigan.gov</p>
<p>Lori Swanson Office of the Minnesota Attorney General 445 Minnesota Street, Suite 1400 St. Paul, MN 55101-2131 Attorney.General@ag.state.mn.us</p>	<p>Jim Hood Mississippi Attorney General's Office 550 High Street Jackson, MS 39201</p>

<p>Josh Hawley Missouri Attorney General's Office Supreme Court Building 207 W. High St. P.O. Box 899 Jefferson City, MO 65102 attorney.general@ago.mo.gov</p>	<p>Tim Fox Office of the Montana Attorney General Justice Building, Third Floor 215 North Sanders P.O. Box 201401 Helena, MT 59620-1401 contactdoj@mt.gov</p>
<p>Montana Office of Consumer Protection P. O. Box 200151 Helena, MT 59620-0151 contactocp@mt.gov</p>	<p>Doug Peterson Nebraska Attorney General's Office 2115 State Capitol P.O. Box 98920 Lincoln, NE 68509 ago.consumer@nebraska.gov</p>
<p>Adam Paul Laxalt Office of the Nevada Attorney General 100 North Carson Street Carson City, NV 89701 AgInfo@ag.nv.gov</p>	<p>Gordon J. MacDonald New Hampshire Department of Justice 33 Capitol Street Concord, NH 03301 attorneygeneral@doj.nh.gov</p>
<p>Christopher S. Porrino Office of the New Jersey Attorney General RJ Hughes Justice Complex 25 Market Street, Box 080 Trenton, NJ 08625-0080 databreach@cyber.nj.gov</p>	<p>Hector Balderas Office of the New Mexico Attorney General 408 Galisteo Street Villagra Building Santa Fe, NM 87501</p>
<p>Eric T. Schneiderman Office of the New York Attorney General The Capitol Albany, NY 12224-0341</p>	<p>Josh Stein North Carolina Attorney General's Office 9001 Mail Service Center Raleigh, NC 27699-9001</p>
<p>Wayne Stenehjem North Dakota Attorney General's Office 600 E. Boulevard Ave. Dept. 125 Bismarck, ND 58505 ndag@nd.gov</p>	<p>Mike DeWine Ohio Attorney General's Office 30 E. Broad Street, 14th Floor Columbus, OH 43215</p>
<p>Mike Hunter Oklahoma Office of the Attorney General 313 NE 21st Street Oklahoma City, OK 73105</p>	<p>Ellen F. Rosenblum Office of the Oregon Attorney General Oregon Department of Justice 1162 Court Street, NE Salem, OR 97301-4096</p>

<p>Josh Shapiro Pennsylvania Office of Attorney General 16th Floor, Strawberry Square Harrisburg, PA 17120</p>	<p>Puerto Rico Departamento de Asuntos del Consumidor Ave. José De Diego, Pda. 22 Centro Gubernamental Minillas Edificio Torre Norte, Piso 7 San Juan, PR 00940 servicio@daco.pr.gov</p>
<p>Peter F. Kilmartin Office of the Rhode Island Attorney General 150 South Main Street Providence, RI 02903</p>	<p>Alan Wilson Office of the South Carolina Attorney General P.O. Box 11549 Columbia, SC 29211</p>
<p>Consumer Protection Division of the Department of Consumer Affairs P.O. Box 5757 Columbia, SC 29250</p>	<p>Marty J. Jackley South Dakota Attorney General's Office 1302 East Highway 14, Suite 1 Pierre, SD 57501-8501 consumerhelp@state.sd.us</p>
<p>Herbert H. Slatery, III Office of the Tennessee Attorney General and Reporter P.O. Box 20207 Nashville, TN 37202-0207</p>	<p>Ken Paxton Office of the Texas Attorney General P.O. Box 12548 Austin, TX 78711-2548</p>
<p>Sean D. Reyes Utah Office of the Attorney General Utah State Capitol Complex 350 N. State St., Suite 230 Salt Lake City, UT 84114-2320 uag@agutah.gov</p>	<p>TJ Donovan Vermont Attorney General's Office 109 State Street Montpelier, VT 05609-1001 ago.cap@vermont.gov</p>
<p>Mark R. Herring Office of the Virginia Attorney General 202 North Ninth Street Richmond, VA 23219</p>	<p>Bob Ferguson Washington State Office of the Attorney General 1125 Washington St SE P.O. Box 40100 Olympia, WA 98504-0100 SecurityBreach@atg.wa.gov</p>

<p>Patrick Morrissey Office of the West Virginia Attorney General State Capitol Complex Bldg. 1, Room E-26 Charleston, WV 25305 consumer@wvago.gov</p>	<p>Brad Schimel Office of the Wisconsin Attorney General Wisconsin Department of Justice P.O. Box 7857 Madison, WI 53707-7857</p>
<p>Peter K. Michael Wyoming Attorney General's Office Kendrick Building 2320 Capitol Avenue Cheyenne, WY 82002 ag.consumer@wyo.gov</p>	

Exhibit B – Approximate Number of Potentially Impacted Residents

Updated: October 12, 2017

Maryland – Approximately 3,007,916



P.O. Box 105054
Atlanta, GA 30348

Name
Street
City, State Zip

October 13, 2017

NOTICE OF DATA BREACH

Dear Customer:

This letter follows up on the cybersecurity incident Equifax announced on September 7, 2017. At Equifax, our priorities with regard to this incident are transparency and continuing to provide timely, reassuring support to every consumer. You are receiving this letter because you are one of the 2.5 million additional potentially impacted U.S. consumers that has personal information that was potentially exposed, as described below.

What Happened

On July 29, 2017, Equifax discovered that criminals exploited a U.S. website application vulnerability to gain access to certain files. Upon discovery, we acted immediately to stop the intrusion. The company promptly engaged a leading, independent cybersecurity firm which has been conducting a comprehensive forensic review to determine the scope of the intrusion, including the specific data impacted. Equifax also reported the criminal access to law enforcement and continues to work with authorities. Based on the company's investigation, the unauthorized access occurred from mid-May through July 2017.

On September 7, 2017 Equifax notified U.S. consumers of the data security incident, including that approximately 143 million U.S. consumers were impacted. On October 2, 2017, following the completion of the forensic portion of the investigation of the incident, Equifax announced that the review determined that approximately 2.5 million additional U.S. consumers were potentially impacted. To minimize confusion, you are receiving this letter because you are one of the 2.5 million additional potentially impacted U.S. consumers.

What Information Was Involved

Most of the consumer information accessed includes names, Social Security numbers, birth dates, addresses, and in some instances, driver's license numbers. In addition to this notice, Equifax will send you a direct mail notice if your credit card number was impacted. We have found no evidence of unauthorized access to Equifax's core consumer or commercial credit reporting databases.

What We Are Doing

Upon learning of this incident, Equifax took steps to stop the intrusion, and engaged an independent cybersecurity firm to forensically investigate and determine the scope. Equifax also engaged the cybersecurity firm to conduct an assessment and provide recommendations on steps that can be taken to help prevent this type of incident from happening again.

Equifax is focused on consumer protection and has established a dedicated website, www.equifaxsecurity2017.com to help consumers. We are also offering free identity theft protection and credit file monitoring to all U.S. consumers, even if a consumer is not impacted by this incident. This offering, called TrustedID Premier, includes 3-Bureau credit monitoring of your Equifax, Experian and TransUnion credit reports; copies of your Equifax credit report; the ability to lock and unlock your Equifax credit report; identity theft insurance; and Internet scanning for your Social Security number - all complimentary to U.S. consumers for one year. To find out more information on this complimentary offer and to sign up, please click on the tab "What Can I Do" on the dedicated website. You must complete the enrollment process by January 31, 2018.

In addition, by January 31, 2018, Equifax will offer a new service allowing all consumers the option of controlling access to their personal credit data. The service we are developing will let consumers easily lock and unlock access to their Equifax credit files -- for free, for life.

What You Can Do

In addition to enrolling in identity theft protection and credit file monitoring, please see the "Identity Theft Prevention Tips" and State Information below. This information provides additional steps you can take, including how to obtain a free copy of your credit report and place a fraud alert and/or credit freeze on your credit report. In addition, please monitor your account statements and report any unauthorized charges to your credit card companies and financial institutions.

For More Information

Equifax is committed to ensuring that your personal information is protected, and we apologize to you for the concern and frustration this incident causes. If you have additional questions, please call our dedicated call center at 866-447-7559, available from 7:00 a.m. to 1:00 a.m. Eastern time, seven days a week. Si usted tiene preguntas, por favor llama nuestro centro de llamadas que está abierto durante los siete días de la semana desde las 7:00 a.m. hasta 1:00 a.m. hora de la costa este: 866-447-7559.

Sincerely,

Equifax Inc.

Identity Theft Prevention Tips

We recommend that you remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your credit reports. You may obtain a free copy of your credit report from each company listed below once every 12 months by requesting your report online at www.annualcreditreport.com, calling toll-free 1-877-322-8228, or mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting any of the credit reporting agencies below:

Equifax
PO Box 740241
Atlanta, GA 30374
www.equifax.com
888-766-0008

Experian
PO Box 9554
Allen, TX 75013
www.experian.com
888-397-3742

TransUnion
PO Box 2000
Chester, PA 19016
www.transunion.com
800-680-7289

If you believe you are the victim of identity theft, you should contact the proper law enforcement authorities, including local law enforcement, and you should consider contacting your state attorney general and/or the Federal Trade Commission ("FTC"). You also may contact the FTC to obtain additional information about avoiding identity theft.

Federal Trade Commission, Consumer Response Center
600 Pennsylvania Avenue NW, Washington, DC 20580; 1-877-IDTHEFT (438-4338)
www.ftc.gov/idtheft

State Attorneys General: Information on how to contact your state attorney general may be found at www.naag.org/naag/attorneys-general/whos-my-ag.php.

You may obtain information from the FTC and the credit reporting agencies listed above about placing a fraud alert and/or credit freeze on your credit report.

IF YOU ARE A MARYLAND RESIDENT

You may obtain information about avoiding identity theft from the Maryland Attorney General's Office. This office can be reached at:

Office of the State of Maryland Attorney General
200 St. Paul Place Baltimore, MD 21202; 1-888-743-0023
www.marylandattorneygeneral.gov

IF YOU ARE A MASSACHUSETTS RESIDENT

Under Massachusetts law, you also have the right to obtain a police report in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it. You may also consider placing a fraud alert message or security freeze on your credit file by calling the toll-free telephone numbers for each of the three national consumer credit reporting agencies listed above. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit, mortgages, employment, housing or other services.

If you have been a victim of identity theft and you provide the credit reporting agency with a valid police report, it cannot charge you to place, lift or remove a security freeze. In all other cases, a credit reporting agency may charge you up to \$5.00 each to place, temporarily lift, or permanently remove a security freeze. To place a security freeze on your credit file, you must send a written request to **each** of the three national consumer reporting agencies listed above by regular, certified or overnight mail. In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address such as a current utility bill or telephone bill;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft;
8. If you are not a victim of identity theft, include payment by check, money order, or credit card (Visa, MasterCard, American Express or Discover only). Do not send cash through the mail.

The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password, or both, that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and social security number) **and** the PIN number or password provided to you when you placed the security freeze as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and social security number) **and** the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.

IF YOU ARE A NEW MEXICO RESIDENT

Under New Mexico law, you also have the right to obtain a police report in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it. You may also consider placing a fraud alert message or security freeze on your credit file by calling the toll-free telephone numbers for each of the three national consumer credit reporting agencies listed above. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit, mortgages, employment, housing or other services.

If you have been a victim of identity theft and you provide the credit reporting agency with a valid police

report, it cannot charge you to place, lift or remove a security freeze. Alternatively, if you are over the age of 65, then the fee will also be waived. In all other cases, a credit reporting agency may charge you up to \$10.00 each to place, temporarily lift, or permanently remove a security freeze. To place a security freeze on your credit file, you must send a written request to **each** of the three national consumer reporting agencies listed above by regular, certified or overnight mail. In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address such as a current utility bill or telephone bill;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft;
8. If you are not a victim of identity theft, include payment by check, money order, or credit card (Visa, MasterCard, American Express or Discover only). Do not send cash through the mail.

The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password, or both, that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and Social Security number) **and** the PIN number or password provided to you when you placed the security freeze as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and Social Security number) **and** the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.

IF YOU ARE A NORTH CAROLINA RESIDENT

You may obtain information about avoiding identity theft from the North Carolina Attorney General's Office. This office can be reached at:

North Carolina Attorney General's Office
9001 Mail Service Center Raleigh, NC 27699-9001; 919-716-6400
www.ncdoj.gov

IF YOU ARE A RHODE ISLAND RESIDENT

You may obtain information about avoiding identity theft from the Rhode Island Attorney General's Office. This office can be reached at:

Office of the State of Rhode Island Attorney General

150 South Main Street Providence, RI 02903; 401-274-4400

www.riag.ri.gov

Under Rhode Island law, you also have the right to obtain a police report in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it. You may also consider placing a fraud alert message or security freeze on your credit file by calling the toll-free telephone numbers for each of the three national consumer credit reporting agencies listed above. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit, mortgages, employment, housing or other services.

If you have been a victim of identity theft and you provide the credit reporting agency with a valid police report, it cannot charge you to place, lift or remove a security freeze. Alternatively, if you are over the age of 65, then the fee will also be waived. In all other cases, a credit reporting agency may charge you up to \$10.00 each to place, temporarily lift, or permanently remove a security freeze. To place a security freeze on your credit file, you must send a written request to **each** of the three national consumer reporting agencies listed above by regular, certified or overnight mail. In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address such as a current utility bill or telephone bill;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft;
8. If you are not a victim of identity theft, include payment by check, money order, or credit card (Visa, MasterCard, American Express or Discover only). Do not send cash through the mail.

The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password, or both, that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and Social Security number) **and** the PIN number or password provided to you when you placed the security freeze as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and Social Security number) **and** the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.

IN THE CIRCUIT COURT FOR Baltimore City

(City or County)

CIVIL - NON-DOMESTIC CASE INFORMATION REPORT**DIRECTIONS**

Plaintiff: This Information Report must be completed and attached to the complaint filed with the Clerk of Court unless your case is exempted from the requirement by the Chief Judge of the Court of Appeals pursuant to Rule 2-111(a).

Defendant: You must file an Information Report as required by Rule 2-323(h).

THIS INFORMATION REPORT CANNOT BE ACCEPTED AS A PLEADING

FORM FILED BY: <input checked="" type="checkbox"/> PLAINTIFF <input type="checkbox"/> DEFENDANT		CASE NUMBER _____
CASE NAME: <u>Patricia M. Benway</u>		vs. <u>Equifax Inc.</u> (Clerk to Insert)
PARTY'S NAME: <u>Patricia M. Benway</u>		PHONE: _____
PARTY'S ADDRESS: <u>1178 Anis Squam Harbour, Pasadena, MD 21122-2554</u>		
PARTY'S E-MAIL: _____		
If represented by an attorney:		
PARTY'S ATTORNEY'S NAME: <u>Martin E. Wolf</u>		PHONE: <u>(410) 825-2300</u>
PARTY'S ATTORNEY'S ADDRESS: <u>100 W Pennsylvania Ave., Suite 100, Towson MD 21204</u>		
PARTY'S ATTORNEY'S E-MAIL: <u>mwolf@GWChrm.com</u>		
JURY DEMAND? <input type="checkbox"/> Yes <input type="checkbox"/> No		
RELATED CASE PENDING? <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No If yes, Case #(s), if known: _____		
ANTICIPATED LENGTH OF TRIAL?: _____ hours _____ days		
PLEADING TYPE		
New Case: <input checked="" type="checkbox"/> Original <input type="checkbox"/> Administrative Appeal <input type="checkbox"/> Appeal		
Existing Case: <input type="checkbox"/> Post-Judgment <input type="checkbox"/> Amendment		
If filing in an existing case, skip Case Category/ Subcategory section - go to Relief section.		
IF NEW CASE: CASE CATEGORY/SUBCATEGORY (Check one box.)		

TORTS	<input type="checkbox"/> Government Insurance	PUBLIC LAW	<input type="checkbox"/> Constructive Trust
<input type="checkbox"/> Asbestos	<input type="checkbox"/> Product Liability	<input type="checkbox"/> Attorney Grievance	<input type="checkbox"/> Contempt
<input type="checkbox"/> Assault and Battery	PROPERTY	<input type="checkbox"/> Bond Forfeiture Remission	<input type="checkbox"/> Deposition Notice
<input type="checkbox"/> Business and Commercial	<input type="checkbox"/> Adverse Possession	<input type="checkbox"/> Civil Rights	<input type="checkbox"/> Dist Ct Mtn Appeal
<input type="checkbox"/> Conspiracy	<input type="checkbox"/> Breach of Lease	<input type="checkbox"/> County/Mncpl Code/Ord	<input type="checkbox"/> Financial
<input type="checkbox"/> Conversion	<input type="checkbox"/> Detinue	<input type="checkbox"/> Election Law	<input type="checkbox"/> Grand Jury/Petit Jury
<input type="checkbox"/> Defamation	<input type="checkbox"/> Distress/Distrain	<input type="checkbox"/> Eminent Domain/Condemn.	<input type="checkbox"/> Miscellaneous
<input type="checkbox"/> False Arrest/Imprisonment	<input type="checkbox"/> Ejectment	<input type="checkbox"/> Environment	<input type="checkbox"/> Perpetuate Testimony/Evidence
<input type="checkbox"/> Fraud	<input type="checkbox"/> Forcible Entry/Detainer	<input type="checkbox"/> Error Coram Nobis	<input type="checkbox"/> Prod. of Documents Req.
<input type="checkbox"/> Lead Paint - DOB of Youngest Plt: _____	<input type="checkbox"/> Foreclosure	<input type="checkbox"/> Habeas Corpus	<input type="checkbox"/> Receivership
<input type="checkbox"/> Loss of Consortium	<input type="checkbox"/> Commercial	<input type="checkbox"/> Mandamus	<input type="checkbox"/> Sentence Transfer
<input type="checkbox"/> Malicious Prosecution	<input type="checkbox"/> Residential	<input type="checkbox"/> Prisoner Rights	<input type="checkbox"/> Set Aside Deed
<input type="checkbox"/> Malpractice-Medical	<input type="checkbox"/> Currency or Vehicle	<input type="checkbox"/> Public Info. Act Records	<input type="checkbox"/> Special Adm. - Atty
<input type="checkbox"/> Malpractice-Professional	<input type="checkbox"/> Deed of Trust	<input type="checkbox"/> Quarantine/Isolation	<input type="checkbox"/> Subpoena Issue/Quash
<input type="checkbox"/> Misrepresentation	<input type="checkbox"/> Land Installments	<input type="checkbox"/> Writ of Certiorari	<input type="checkbox"/> Trust Established
<input type="checkbox"/> Motor Tort	<input type="checkbox"/> Lien	EMPLOYMENT	<input type="checkbox"/> Trustee Substitution/Removal
<input type="checkbox"/> Negligence	<input type="checkbox"/> Mortgage	<input type="checkbox"/> ADA	<input type="checkbox"/> Witness Appearance-Compel
<input type="checkbox"/> Nuisance	<input type="checkbox"/> Right of Redemption	<input type="checkbox"/> Conspiracy	PEACE ORDER
<input type="checkbox"/> Premises Liability	<input type="checkbox"/> Statement Condo	<input type="checkbox"/> EEO/HR	<input type="checkbox"/> Peace Order
<input type="checkbox"/> Product Liability	<input type="checkbox"/> Forfeiture of Property / Personal Item	<input type="checkbox"/> FLSA	EQUITY
<input type="checkbox"/> Specific Performance	<input type="checkbox"/> Fraudulent Conveyance	<input type="checkbox"/> FMLA	<input type="checkbox"/> Declaratory Judgment
<input type="checkbox"/> Toxic Tort	<input type="checkbox"/> Landlord-Tenant	<input type="checkbox"/> Workers' Compensation	<input type="checkbox"/> Equitable Relief
<input type="checkbox"/> Trespass	<input type="checkbox"/> Lis Pendens	<input type="checkbox"/> Wrongful Termination	<input type="checkbox"/> Injunctive Relief
<input type="checkbox"/> Wrongful Death	<input type="checkbox"/> Mechanic's Lien	INDEPENDENT PROCEEDINGS	<input type="checkbox"/> Mandamus
CONTRACT	<input type="checkbox"/> Ownership	<input type="checkbox"/> Assumption of Jurisdiction	OTHER
<input type="checkbox"/> Asbestos	<input type="checkbox"/> Partition/Sale in Lieu	<input type="checkbox"/> Authorized Sale	<input type="checkbox"/> Accounting
<input type="checkbox"/> Breach	<input type="checkbox"/> Quiet Title	<input type="checkbox"/> Attorney Appointment	<input type="checkbox"/> Friendly Suit
<input type="checkbox"/> Business and Commercial	<input type="checkbox"/> Rent Escrow	<input type="checkbox"/> Body Attachment Issuance	<input type="checkbox"/> Grantor in Possession
<input type="checkbox"/> Confessed Judgment	<input type="checkbox"/> Return of Seized Property	<input type="checkbox"/> Commission Issuance	<input type="checkbox"/> Maryland Insurance Administration
(Cont'd)	<input type="checkbox"/> Right of Redemption		<input checked="" type="checkbox"/> Miscellaneous
<input type="checkbox"/> Construction	<input type="checkbox"/> Tenant Holding Over		<input type="checkbox"/> Specific Transaction
<input type="checkbox"/> Debt			<input type="checkbox"/> Structured Settlements
<input type="checkbox"/> Fraud			

IF NEW OR EXISTING CASE: RELIEF (Check All that Apply)

- | | | | |
|--|---|--|---|
| <input type="checkbox"/> Abatement | <input type="checkbox"/> Earnings Withholding | <input type="checkbox"/> Judgment-Interest | <input type="checkbox"/> Return of Property |
| <input type="checkbox"/> Administrative Action | <input type="checkbox"/> Enrollment | <input type="checkbox"/> Judgment-Summary | <input type="checkbox"/> Sale of Property |
| <input type="checkbox"/> Appointment of Receiver | <input type="checkbox"/> Expungement | <input type="checkbox"/> Liability | <input type="checkbox"/> Specific Performance |
| <input type="checkbox"/> Arbitration | <input type="checkbox"/> Findings of Fact | <input type="checkbox"/> Oral Examination | <input type="checkbox"/> Writ-Error Coram Nobis |
| <input type="checkbox"/> Asset Determination | <input type="checkbox"/> Foreclosure | <input type="checkbox"/> Order | <input type="checkbox"/> Writ-Execution |
| <input type="checkbox"/> Attachment b/f Judgment | <input type="checkbox"/> Injunction | <input type="checkbox"/> Ownership of Property | <input type="checkbox"/> Writ-Garnish Property |
| <input type="checkbox"/> Cease & Desist Order | <input type="checkbox"/> Judgment-Affidavit | <input type="checkbox"/> Partition of Property | <input type="checkbox"/> Writ-Garnish Wages |
| <input type="checkbox"/> Condemn Bldg | <input type="checkbox"/> Judgment-Attorney Fees | <input type="checkbox"/> Peace Order | <input type="checkbox"/> Writ-Habeas Corpus |
| <input type="checkbox"/> Contempt | <input type="checkbox"/> Judgment-Confessed | <input type="checkbox"/> Possession | <input type="checkbox"/> Writ-Mandamus |
| <input type="checkbox"/> Court Costs/Fees | <input type="checkbox"/> Judgment-Consent | <input type="checkbox"/> Production of Records | <input type="checkbox"/> Writ-Possession |
| <input type="checkbox"/> Damages-Compensatory | <input type="checkbox"/> Judgment-Declaratory | <input type="checkbox"/> Quarantine/Isolation Order | |
| <input type="checkbox"/> Damages-Punitive | <input type="checkbox"/> Judgment-Default | <input type="checkbox"/> Reinstatement of Employment | |

If you indicated *Liability* above, mark one of the following. This information is not an admission and may not be used for any purpose other than Track Assignment.

☐ Liability is conceded. ☐ Liability is not conceded, but is not seriously in dispute. ☐ Liability is seriously in dispute.

MONETARY DAMAGES (Do not include Attorney's Fees, Interest, or Court Costs)

☐ Under \$10,000 ☐ \$10,000 - \$30,000 ☐ \$30,000 - \$100,000 ☒ Over \$100,000

☐ Medical Bills \$ _____ ☐ Wage Loss \$ _____ ☐ Property Damages \$ _____

ALTERNATIVE DISPUTE RESOLUTION INFORMATION

Is this case appropriate for referral to an ADR process under Md. Rule 17-101? (Check all that apply)

A. Mediation ☒ Yes ☐ No C. Settlement Conference ☒ Yes ☐ No
B. Arbitration ☐ Yes ☒ No D. Neutral Evaluation ☐ Yes ☒ No

SPECIAL REQUIREMENTS

- ☐ If a Spoken Language Interpreter is needed, check here and attach form CC-DC-041
- ☐ If you require an accommodation for a disability under the Americans with Disabilities Act, check here and attach form CC-DC-049

ESTIMATED LENGTH OF TRIAL

With the exception of Baltimore County and Baltimore City, please fill in the estimated **LENGTH OF TRIAL**.

(Case will be tracked accordingly)

- ☐ 1/2 day of trial or less ☐ 3 days of trial time
☐ 1 day of trial time ☐ More than 3 days of trial time
☐ 2 days of trial time

BUSINESS AND TECHNOLOGY CASE MANAGEMENT PROGRAM

For all jurisdictions, if Business and Technology track designation under Md. Rule 16-308 is requested, attach a duplicate copy of complaint and check one of the tracks below.

- ☐ Expedited- Trial within 7 months of Defendant's response ☐ Standard - Trial within 18 months of Defendant's response

EMERGENCY RELIEF REQUESTED

**COMPLEX SCIENCE AND/OR TECHNOLOGICAL CASE
MANAGEMENT PROGRAM (ASTAR)**

*FOR PURPOSES OF POSSIBLE SPECIAL ASSIGNMENT TO ASTAR RESOURCES JUDGES under
Md. Rule 16-302, attach a duplicate copy of complaint and check whether assignment to an ASTAR is requested.*

☐ Expedited - Trial within 7 months of
Defendant's response

☐ Standard - Trial within 18 months of
Defendant's response

***IF YOU ARE FILING YOUR COMPLAINT IN BALTIMORE CITY, OR BALTIMORE COUNTY,
PLEASE FILL OUT THE APPROPRIATE BOX BELOW.***

CIRCUIT COURT FOR BALTIMORE CITY (CHECK ONLY ONE)

- | | |
|--|---|
| <input type="checkbox"/> Expedited | Trial 60 to 120 days from notice. Non-jury matters. |
| <input type="checkbox"/> Civil-Short | Trial 210 days from first answer. |
| <input type="checkbox"/> Civil-Standard | Trial 360 days from first answer. |
| <input checked="" type="checkbox"/> Custom | Scheduling order entered by individual judge. |
| <input type="checkbox"/> Asbestos | Special scheduling order. |
| <input type="checkbox"/> Lead Paint | Fill in: Birth Date of youngest plaintiff _____. |
| <input type="checkbox"/> Tax Sale Foreclosures | Special scheduling order. |
| <input type="checkbox"/> Mortgage Foreclosures | No scheduling order. |

CIRCUIT COURT FOR BALTIMORE COUNTY

- | | |
|---|--|
| <input type="checkbox"/> Expedited
(Trial Date-90 days) | Attachment Before Judgment, Declaratory Judgment (Simple),
Administrative Appeals, District Court Appeals and Jury Trial Prayers,
Guardianship, Injunction, Mandamus. |
| <input type="checkbox"/> Standard
(Trial Date-240 days) | Condemnation, Confessed Judgments (Vacated), Contract, Employment
Related Cases, Fraud and Misrepresentation, International Tort, Motor Tort,
Other Personal Injury, Workers' Compensation Cases. |
| <input type="checkbox"/> Extended Standard
(Trial Date-345 days) | Asbestos, Lender Liability, Professional Malpractice, Serious Motor Tort or
Personal Injury Cases (medical expenses and wage loss of \$100,000, expert
and out-of-state witnesses (parties), and trial of five or more days), State
Insolvency. |
| <input type="checkbox"/> Complex
(Trial Date-450 days) | Class Actions, Designated Toxic Tort, Major Construction Contracts, Major
Product Liabilities, Other Complex Cases. |

October 5, 2017

Date

100 W. Pennsylvania Ave., Suite 100

Address

Towson

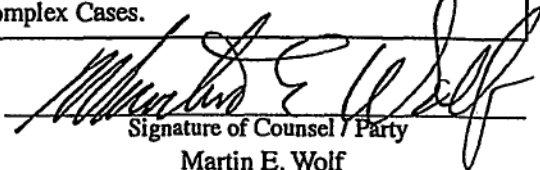
MD

21204

City

State

Zip Code


Signature of Counsel / Party

Martin E. Wolf

Printed Name