CHRISTENSEN YOUNG & ASSOCIATES, PLLC
STEVEN A. CHRISTENSEN (#5190)
CAMERON S. CHRISTENSEN (#16015)
9980 S. 300 W. Ste. 200
Sandy, Utah 84070
Tel: (801) 676-6447
Email: steven@christensenyounglaw.com
cameron@christensenyounglaw.com

MORGAN & MORGAN
COMPLEX LITIGATION GROUP
John A. Yanchunis, Esquire [To be admitted *Pro Hac Vice*]
Jean S. Martin, Esquire [To be admitted *Pro Hac Vice*]
Ryan J. McGee, Esquire [To be admitted *Pro Hac Vice*]
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
Tel.: (813) 223-5505
Email: jyanchunis@ForThePeople.com
jsm@jsmlawoffice.com
rmcgee@ForThePeople.com

Attorneys for Plaintiff and the Putative Class

IN THE UNITED STATES DISTRICT COURT FOR THE DISTRICT OF UTAH

SHOWNEEN HALL, on behalf of herself and other persons similarly situated, **Plaintiff** **v.** **MYHERITAGE, LTD., an Israeli corporation, and MYHERITAGE (USA), INC., a Delaware corporation,** **Defendants.**	**COMPLAINT and DEMAND FOR JURY TRIAL** Civil No.: 2:18-cv-00721 EJF Judge: Evelyn J. Furse

Plaintiff, Showneen Hall, by way of Complaint on behalf of herself and others similarly situated, individually and as class representative, upon information and belief, except for the allegations concerning Plaintiff's own actions, says as follows:

NATURE OF THE ACTION

1. This is a class-action Complaint brought by Plaintiff, Showneen Hall ("Plaintiff") on her own behalf and on behalf of all others similarly situated against Defendants, MyHeritage, Ltd. ("MHL"), and MyHeritage (USA), Inc. ("MHI"), (collectively "Defendants"), to: 1) obtain declaratory, injunctive, and monetary relief for a class of individuals against Defendants for their failure to safeguard users' Protected Health Information ("PHI") and Personal Identifying Information ("PII"), which Defendants collected from Plaintiff and Class Members (collectively "Private Information"); 2) for failing to provide timely, accurate, and adequate notice to Plaintiff and other Class Members that their Private Information had been stolen; and 3) for failing to provide timely, accurate, and adequate notice of precisely what types of information were stolen.

PARTIES, JURISDICTION, AND VENUE

2. Plaintiff, Showneen Hall, is an adult individual residing in Tampa, Florida, who found out about the data breach from Defendants in their June 4, 2018, public announcement that her username and password information protecting her Private Information was accessed and stored by unauthorized persons.

3. Defendant MHL is a business entity incorporated under the laws of Israel with a headquarters located Tel Aviv, Israel. Upon information and belief, MHL is the parent company for MHI.

4. Defendant MHI is a corporation incorporated under the laws of Delaware with a headquarters located at 2975 Executive Parkway, Suite 310, Lehi, Utah 84043. Upon information and belief, MHI is a subsidiary of MHL.

5. Defendants operate "the leading global destination for discovering, preserving and sharing family history. [Defendants'] platform and DNA kits make it easy for anyone, anywhere to embark on a meaningful journey into their past and treasure their family stories for generations to come." [1]

6. This Court has jurisdiction over this action pursuant to the Class Action Fairness Act ("CAFA"), 28 U.S.C. § 1332(d), because the aggregate amount in controversy exceeds $5,000,000, exclusive of interests and costs, there are more than 100 class members, and at least one class member is a citizen of a state different from Defendants and is a citizen of a foreign state. The Court also has supplemental jurisdiction over the state law claims pursuant to 28 U.S.C. § 1367.

7. Venue is proper under 28 U.S.C. § 1391(c) because Defendants are corporations that do business in, and are subject to personal jurisdiction in, this District. Venue is also proper because a substantial part of the events or omissions giving rise to the claims in this action occurred in or emanated from this District, including the decisions made by Defendants to aggregate and collect Plaintiff's and the Class members' information.

FACTUAL ALLEGATIONS

A. MyHeritage's Services and Products

8. Defendants, through their operation of the MyHeritage websites, are a leading provider for discovering, preserving, and sharing family history, as well as DNA genealogy.[2]

[1] MyHeritage, *About Us*, https://www.myheritage.com/about-myheritage/ (last visited June 13, 2018).
[2] *Id.*

9. Defendants offer consumers the family history and DNA genealogy services and products through, *inter alia*, their website, https://www.myheritage.com/ where patients can review and explore their family history and DNA genealogy.

10. Defendants, in marketing their products and services, tout not only the security of the service, but encourage consumers to add information to the PII and PHI already on file with Defendants, including encouraging consumers to add familial history, to include maiden names, and other intimate details of a consumer's past,[3] all of which are typically used for password reminders and resets with financial institutions, healthcare providers, and other companies with which consumers entrust PII and PHI.

11. Despite storing sensitive Private Information that they knew or should have known was valuable to and vulnerable to cyber attackers, Defendants failed to take adequate measures that could have protected user's Private Information.

12. On or about June 4, 2018 Defendants announced that:

> Today, June 4, 2018 at approximately 1pm EST, MyHertiage's Chief Information Security Officer received a message from a security researcher that he had found a file named myheritage containing email addresses and hashed passwords, on a private server outside of MyHeritage. Our Information Security Team received the file from the security researcher, reviewed it, and confirmed that its contents originated from MyHeritage and included all the email addresses of users who signed up to MyHeritage up to October 26, 2017, and their hashed passwords.[4]

(hereinafter, the "Data Breach").

[3] MyHeritage, *New Historical Records Added in May 2018*, June 3, 2018 https://blog.myheritage.com/2018/06/new-historical-records-added-in-may-2018/.

[4] MyHeritage, *MyHeritage Statement About a Cybersecurity Incident*, June 4, 2018, https://blog.myheritage.com/2018/06/myheritage-statement-about-a-cybersecurity-incident/ (last visited June 12, 2018).

B. Consumers Rely on Defendants' Private Information Security Practices

13. Defendants maintain a Privacy Policy on their website ("Privacy Policy"),[5] which provides, in relevant part:

> Much of the personal information on our Website is uploaded by users for their own personal and private purposes. We recognize the sensitivity and confidentiality of information that may be disclosed by users in registering, making purchases from our Website, performing their family history research, performing DNA testing and receiving genetic analysis, and we are firmly committed to protecting your privacy.
>
> **What personal information does the Website collect from you or about you?**
>
> We collect information we believe is necessary for our legitimate business interests, including to provide you with the Service. Here is a list of the type of personal information we request, collect or you provide:
>
> *i) Name, Contact Information and Payment Details:*
>
> When you sign up for the Service, we ask for your name, gender and email address, as well as birth year and country. The birth year is collected to ensure that you comply with the Terms and Conditions with regards to underage and minor users. Users who are underage (below age 13, and in some countries, below the age 14, and with respect to the DNA Services, below the age of 18) must not use the Website, and users who are minors (below age 18) must obtain the written consent of a parent or guardian before using the Website. See the **Terms and Conditions** in this regard. The country is collected so that we can comply with local laws and regulations in your country of residence.
>
> In addition we will need to know your postal address, phone number and payment details to facilitate payment and fulfillment for any subscription or purchases you may choose to make through the Website.
>
> *ii) Your Family and Others:*
>
> You may also post additional personal information about yourself

[5] MyHeritage, *Privacy Policy*, https://www.myheritage.com/FP/Company/popup.php?p=privacy_policy, (last visited June 12, 2018).

and others in the course of doing your family research on the Website, e.g., adding a photo to a family tree. Personal information entered in the course of building a family tree may include any of the following:

- Names
- Gender
- Relationships
- Dates and places of events (e.g., birth, death, marriage, divorce, immigration, etc.)
- Photos, documents, video files, audio files and other media
- Email addresses, addresses and contact information and more.

iii) DNA samples, DNA Results and DNA Reports:

By submitting DNA samples to us and/or DNA Results to the Website, you grant us a royalty-free, world-wide license to use your DNA samples, the DNA Results and the resulting DNA Reports, and any DNA samples and/or DNA Results you submit for any person from whom you obtained legal authorization and the resulting DNA Reports, to the minimum extent necessary to allow us to provide the Service to you. The license you grant to us is not perpetual, and it is revocable as you are able at any time to delete your DNA Results and DNA Reports permanently from the Website and to have us destroy your DNA samples.

DNA related information is generated and stored on the Website when you use the DNA Services, whether through direct submission of a DNA sample to MyHeritage or by submitting to the Website, DNA Results generated by another DNA testing service.

The DNA information includes:

- DNA samples you submit to us;
- DNA Results resulting from the DNA samples;
- DNA Results submitted by you to the Website; and
- DNA Reports generated from the DNA Results

All DNA samples are stored at our testing lab and may be kept by us unless or until circumstances require us to destroy the DNA sample, which you can request at any time by contacting us using the contact details below, or it is no longer suitable for testing purposes. We may store the samples for additional genetic testing (i.e., we may be able to provide more detailed and accurate DNA

Results, DNA Reports and other outputs by additional genetic testing in the future, subject to your explicit approval).

[…]

When you provide us with any personal information, that personal information may be transferred to and stored by us in our secure data centers which may provide a different level of protection for personal information than in your country of residence. By providing us with personal or genetic information, you specifically consent to the transfer and processing of personal information and its storage in our data centers. We take all adequate security measures to ensure the privacy protection of the personal information provided by you. We place great importance on the security of all personally identifiable information associated with our members. We have implemented commercially reasonable technical, physical and administrative security measures in place to attempt to protect against the loss, misuse, unauthorized access, alteration or disclosure of users' personal information under our control. For example our security and privacy practices are periodically reviewed and enhanced as necessary and only authorized personnel have access to personal information. We use secure server software to encrypt financial information you input before it is sent to us and we only work with labs and third parties who have met and commit to our security standards. While we cannot guarantee that loss, misuse, unauthorized access, alteration or disclosure of personal information will not occur; we use commercially reasonable efforts to prevent this.

[…]

iv) Your Opinions and Comments:

If you participate in discussions on our message boards, or post messages on our blogs or Facebook accounts, we may capture that information.

v) Your Use of the Website:

While you use our Website, we may collect information based on your interaction with our Website or from the devices or computers you use to access the Website, including web log information, page views and IP addresses, all on an anonymized basis.

vi) Survey Answers:

The voluntary Surveys on MyHeritage (the **"Surveys"**) collect, preserve and analyze self-reported information related to physical and other personal traits, demography, household, lifestyle, habits, preferences, hobbies and interests, opinions, family, occupation, health, psychological and cognitive traits and other similar information (collectively, the **"Survey Research Information"**).

vii) Health Family Tree:

The Health Family Tree allows you to enter information concerning health conditions, physical traits and other personal traits about yourself and your immediate family members (collectively, the "Health Family Tree Information").

[…]

Will MyHeritage disclose any of my personal information to third parties?

In no case is the personal information provided by our users sold, licensed or otherwise shared by us with advertisers, sponsors, partners or other third parties. We will never sell or license DNA samples, DNA Results, DNA Reports or any other DNA information, to any third parties without your explicit informed consent, and we will never sell or license such information to insurance companies under any circumstances.

MyHeritage will not disclose any of your personal information except in very limited circumstances which are set out below.

i) In limited circumstances: (a) if required by law, regulatory authorities, legal process or to protect the rights or property of MyHeritage or other users (including outside your country of residence); (b) to enforce our Terms and Conditions; (c) to protect our rights, privacy, safety, confidentiality, reputation or property, and/or that of the MyHeritage Website Group, or others; (d) to prevent fraud or cybercrime; (e) to permit us to pursue available remedies or limit the damages that we may sustain; or (f) to investigate rare cases involving reported abuse of our Privacy Policy.

ii) In an acquisition of MyHeritage: in the event that MyHeritage, or substantially all of its assets or stock are acquired, transferred, disposed of (in whole or part and including in connection with any bankruptcy or similar proceedings), personal information will as a matter of course be one of the transferred assets.

> *iii) To third-party service providers:* Under the protection of appropriate agreements, we use third parties to perform various tasks for us. For example, we use third party platforms to process payments from you or use a specialized DNA lab to extract, process and store your DNA samples. These third-parties are only given access to that information needed to perform their support functions, and are prohibited from using it for other purposes. With respect to processors outside the European Economic Area, we attempt to ensure adequate safeguards for your personal information, as required by applicable law.
>
> *iv) To your DNA Matches:* If you use our DNA Services and DNA Matches are enabled, the DNA Reports will include a list of your potential relatives, based on DNA. Each one of the people who match your DNA will be able to see the amount of DNA they have in common with you and the predicted family relationship between you, and some of your personal information such as your display name, your country of residence, your ethnic estimate and other profile information, depending on your privacy settings.

14. Thus, Defendants collect and store massive amounts of Private Information on their users and utilize this information to maximize profits.

15. Consumers place value in data privacy and security, and they consider it when making decisions regarding their online behavior, especially signing up for an online DNA genealogy analysis site. Plaintiff would not have utilized Defendants' services had she known that Defendants did not take all necessary precautions to secure the Private Information that consumers provide to Defendants.

16. Defendants failed to disclose their negligent and insufficient data security practices and consumers relied on or were misled by these omissions, resulting in Plaintiff's and Class Members' using Defendants services.

17. The technology and medical industry is rife with similar examples of hackers targeting users' Private Information, including the hacks of Anthem[6], Premera[7], and St. Joseph Health System[8] among others, all of which predate the time-frame MyHeritage identified regarding the Data Breach at issue in the present lawsuit.

18. As early as 2014 the FBI alerted healthcare firms that they were the target of hackers, stating "The FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PII)".[9]

19. In fact, just months before the represented date of the breach, Gizmodo reported that DNA testing data was "disturbingly vulnerable to hackers."[10] In its report, Gizmodo noted an upcoming presentation from the 26th USENIX Security Symposium in Vancouver, wherein University of Washington researchers "analyzed the security practices of common, open-source DNA processing programs and found that they were, in general, lacking."[11] This lacking security meant that consumers' DNA and other valuable information was vulnerable to hackers.[12] This Gizmodo report was published on August 10, 2017—less than three months prior to this Data Breach on October 26, 2017.

---

[6] Los Angeles Times, *Anthem is warning consumers about its huge data breach. Here's a translation*, March 6, 2015. http://www.latimes.com/business/la-fi-mh-anthem-is-warning-consumers-20150306-column.html.

[7] New York Times, *Premera Blue Cross Says Data Breach Exposed Medical Data*, March 17, 2015. http://www.nytimes.com/2015/03/18/business/premera-blue-cross-says-data-breach-exposed-medical-data.html?_r=0.

[8] Napa Valley Register, *St. Joseph Health System sued for patient data breach*, April 9, 2012. http://napavalleyregister.com/news/local/st-joseph-health-system-sued-for-patient-data-breach/article_948c0896-82a3-11e1-bed6-0019bb2963f4.html.

[9] Reuters, *FBI Warns Healthcare Firms They are Targeted by Hackers*, August 20, 2014, http://www.reuters.com/article/us-cybersecurity-healthcare-fbi-idUSKBN0GK24U20140820.

[10] Gizmodo, *DNA Testing Data is Disturbingly Vulnerable to Hackers*, August 10, 2017, https://gizmodo.com/dna-testing-data-is-disturbingly-vulnerable-to-hackers-1797695128.

[11] *Id.*

[12] *Id.*

C. Stolen Private Information Is Valuable to Hackers and Thieves

20. It is well known and the subject of many media reports that both Private Health Information and Personal Identify information is highly coveted and a frequent target of hackers. This information is targeted not only for identity theft purposes, but also for committing healthcare fraud, obtaining medical services under another's insurance. A study by Experian found that the "average total cost" of medical identity theft is "about $20,000" per incident, and that a majority of victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[13] Despite well publicized litigation and frequent public announcements of data breaches by medical and technology companies, Defendants opted to maintain an insufficient and inadequate system to protect the PHI and PII of Plaintiff and Class Members.

21. Legitimate organizations and the criminal underground alike recognize the value of PII. Otherwise, they wouldn't aggressively seek or pay for it. For example, in "one of 2013's largest breaches . . . not only did hackers compromise the [card holder data] of three million users, they also took registration data from 38 million users."[14] Similarly, in the Target data breach, in addition to PCI data pertaining to 40,000 credit and debit cards, hackers stole PII pertaining to 70,000 users.

22. Biographical data is also highly sought after by data thieves. "Increasingly, criminals are using biographical data gained from multiple sources to perpetrate more and larger thefts." *Id.* PII data has been stolen and sold by the criminal underground on many occasions in the past, and the accounts of theft and unauthorized access have been the subject of many media

[13] Elinor Mills, *Study: Medical Identity Theft is Costly for Victims*, March 3, 2010, 5:00am PST, available at: https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/.
[14] Verizon 2014 PCI Compliance Report, Available at http://www.cisco.com/c/dam/en_us/solutions/industries/docs/retail/verizon_pci2014.pdf (hereafter "2014 Verizon Report"), at 54.

reports. One form of identity theft, branded "synthetic identity theft," occurs when thieves create new identities by combining real and fake identifying information and then use those identities to open new accounts. "This is where they'll take your Social Security number, my name and address, someone else's birthday and they will combine them into the equivalent of a bionic person," said Adam Levin, Chairman of IDT911, which helps businesses recover from identity theft. Synthetic identity theft is harder to unravel than traditional identity theft, experts said: "It's tougher than even the toughest identity theft cases to deal with because they can't necessarily peg it to any one person." In fact, the fraud might not be discovered until an account goes to collections and a collection agency researches the Social Security number.

23. Unfortunately, and as is alleged below, despite all of this publicly available knowledge of the continued compromises of Private Information in the hands of third parties, such as DNA analysis companies, Defendants' approach at maintaining the privacy of Plaintiff's and Class Members' Private Information was lackadaisical, cavalier, reckless, or at the very least negligent.

D. This Data Breach Will Result in Additional Identity Theft and Identity Fraud.

24. Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the Private Information maintained on their systems.

25. The ramifications of Defendants' failure to keep Plaintiff's and Class Members' data secure are severe. As explained by the Federal Trade Commission:

> Medical identity theft happens when someone steals your personal information and uses it to commit health care fraud. Medical ID thieves may use your identity to get treatment — even surgery — or to bilk insurers by making fake claims. Repairing damage to your good name and credit record can be difficult enough, but

> medical ID theft can have other serious consequences. If a scammer gets treatment in your name, that person's health problems could become a part of your medical record. It could affect your ability to get medical care and insurance benefits, and could even affect decisions made by doctors treating you later on. The scammer's unpaid medical debts also could end up on your credit report.[15]

26. As the FTC recognizes, once identity thieves have personal information, "they can drain your bank account, run up your credit cards, open new utility accounts, or get medical treatment on your health insurance."[16]

27. According to Javelin Strategy and Research, "1 in 4 notification recipients became a victim of identity fraud."[17]

28. It is incorrect to assume that reimbursing a consumer for a financial loss due to fraud makes that individual whole again. On the contrary, after conducting a study, the Department of Justice's Bureau of Justice Statistics ("BJS") found that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems."[18] In fact, the BJS reported, "resolving the problems caused by identity theft [could] take more than a year for some victims." *Id*. at 11.

29. Javelin Strategy and Research reports that losses from identity theft increased to $21 billion in 2013.[19]

---

[15] Federal Trade Commission, *Medical ID Theft: Health Information for Older People*, available at https://www.consumer.ftc.gov/articles/0326-medical-id-theft-health-information-older-people.
[16] U.S. Federal Trade Commission, *Warning Signs of Identity Theft*, available at https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft.
[17] Javelin, *2013 Identity Fraud Report: Data Breaches Becoming a Treasure Trove for Fraudsters*, available at www.javelinstrategy.com/brochure/276, (the "2013 Identity Fraud Report").
[18] U.S. Department of Justice, *Victims of Identity Theft, 2012* (Dec. 2013) at 10, *available at* http://www.bjs.gov/content/pub/pdf/vit12.pdf.
[19] *See generally* 2013 Identity Fraud Report.

30. There may be a time lag between when harm occurs and when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[20]

31. Plaintiff and Class Members now face years of constant surveillance of their financial, personal, and medical records. The Class is incurring and will continue to incur such damages in addition to any fraudulent charges made to their financial accounts or medical insurance, whether or not such charges are ultimately reimbursed by the credit card companies and other financial institutions, such as PayPal.

E. Defendants Failed to Maintain the Confidentiality of Plaintiff's and Class Members' Private Health Information and Continue to Inadequately Secure Plaintiff's and Class Members' Information.

32. Defendant had a duty to maintain the confidentiality of Plaintiff's and Class Members' Private Health Information.

33. Defendants' duties included ensuring Plaintiff's and Class Members' electronic protected health information was not made available or disclosed to unauthorized third persons or processes.

34. Defendants' duties also included protecting against reasonably anticipated threats or hazards to the security of Plaintiff's and Class Members' Private Health Information.

[20] U.S. Government Accountability Office, *Report to Congressional Requesters*, at p.33 (June 2007), *available at* http://www.gao.gov/new.items/d07737.pdf (emphases added).

35. Defendants failed to adequately protect Plaintiff's and Class Members' Private Health Information from the reasonably anticipated threat of hackers gaining access to usernames and password information, thus enabling hackers access to the Private Health Information contained in Defendants' systems.

36. As a result of the Defendants' failure to protect against reasonably anticipated threats, the electronic Private Health Information of Plaintiff and the Class was made available to third persons.

37. Plaintiff and Class Members have a privacy right in their Private Health Information.

38. As a result of Defendants' failure to maintain the confidentiality of Plaintiff's and Class Members' Private Health Information, Plaintiff and Class Members suffered an injury through their a loss of privacy—especially given the sensitive and private nature of DNA.

F. Defendants Have Not Fixed the Flaws in their Security

39. In notifying Plaintiff and Class Members, Defendant indicated that it "set up an Information Security Incident Response Team to investigate the incident," and took "immediate steps to engage a leading, independent cybersecurity firm to conduct comprehensive forensics reviews to determine the scope of the intrusion; and to conduct an assessment and provide *recommendations* on steps that *can* be taken to *help* prevent such an incident from occurring in the future."[21]

40. That representation was designed to create the impression that the flaw in Defendants' security had been repaired and induce Plaintiff and Class Members to continue utilizing Defendants' services.

[21] MyHeritage, *MyHeritage Statement About a Cybersecurity Incident*, June 4, 2018, https://blog.myheritage.com/2018/06/myheritage-statement-about-a-cybersecurity-incident/ (last visited June 12, 2018).

41. Defendants, by virtue of not knowing how the breach occurred, did not fix the flaw which permitted unauthorized access to Plaintiff's and Class Members' Private Information, and have not indicated any efforts to further secure the Private Information subsequent to their June 4, 2018, blog post.

G. Plaintiff and Class Members Suffered Damages

42. Although Defendants claim user's payment information is secure, Plaintiff's PayPal account and financial information was linked to Defendants' site.

43. Since the Data Breach on October 26, 2017, Plaintiff has noticed multiple fraudulent charges on her personal credit report, which includes the financial information and credit cards linked to her PayPal account.

44. Plaintiff has taken preventative measures, including, but not limited to, contacting her financial institutions, as well as PayPal, to address and reverse the fraudulent charges, changing her passwords, and spending additional time monitoring her credit reports.

45. Additionally, Plaintiff, encouraged and compelled by the alleged security and reputation of Defendants' services and products, purchased and submitted the DNA test kit, providing Private Health Information to Defendants, and reasonably expected that PHI would be kept and safeguarded from malicious third-party hackers. After signing up for, receiving, and submitting her DNA test kit, the results were linked to Plaintiff's MyHeritage account, accessible via her username and password, and, upon information and belief, disclosed in the Data Breach.

46. The Data Breach was a direct and proximate result of Defendants' failure to properly safeguard and protect Plaintiff's and Class Members' Private Information from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and the common law, including Defendants' failure to establish and

implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiff's and Class members' Private Information to protect against reasonably foreseeable threats to the security or integrity of such information.

47. Plaintiff's and Class Members' Private Information is private and sensitive in nature and was left inadequately protected by Defendants. Defendants did not obtain Plaintiff's and Class Members' consent to disclose either their Personal Identifying Information or their Private Health Information to any other person as required by applicable law and industry standards.

48. As a direct and proximate result of Defendants' wrongful actions and inaction and the resulting Data Breach, Plaintiff and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and identity fraud, requiring them to take time and effort to mitigate the actual and potential impact of the Data Breach on their lives by, among other things, placing "freezes" or "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring their credit reports and accounts for unauthorized activity.

49. Furthermore, Plaintiff and Class Members have suffered injuries in the loss of privacy through the disclosure of their Private Health Information and/or DNA genealogy reports.

50. Defendants' wrongful actions and inaction directly and proximately caused the theft and dissemination into the public domain of Plaintiff's and Class Members' Private Information, causing them to suffer, and continue to suffer, economic damages and other actual harm for which they are entitled to compensation including:

a. Theft of their personal, medical, and/or financial information;

b. The reputational harms suffered by Defendants' publication of private facts in the form of Plaintiff's and Class Members' DNA;

c. The imminent and certainly impending injury flowing from potential fraud and identity theft posed by their personal and medical information being placed in the hands of criminals;

d. The untimely and inadequate notification of the Data Breach;

e. The improper disclosure of Plaintiff's and Class Members' Private Information;

f. Loss of Privacy;

g. Ascertainable loss in the form of out-of pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach;

h. Ascertainable losses in the form of deprivation of the value of their Personal Identifying Information and Private Health Information, for which there is a well-established national and international market;

i. Overpayments to Defendants for products and services in that a portion of the price paid for such products and services by Plaintiff and Class Members to Defendants was for the costs of reasonable and adequate safeguards and security measures that would protect users' Private Information, which Defendants did not implement and, as a result, Plaintiff and Class Members did not receive what they paid for and were overcharged by Defendants;

j. Defendants continue to inadequately secure Plaintiff's and Class Members' Private Information.

CLASS ACTION ALLEGATIONS

51. This action is brought and may properly proceed as a class action, pursuant to the provisions of Rule 23 of the Federal Rules of Civil Procedure. Plaintiff brings this action on behalf of herself and all others similarly situated. Plaintiff seeks certification of a Class, initially defined as follows:

> **All persons residing in the United States whose Personal Identifying Information and/or Private Health Information was disclosed in the Data Breach announced by Defendants on or about June 4, 2018.**

52. The Class for those whose benefit this action has been brought is so numerous that joinder of all members is impracticable, as Defendants have indicated they believe more than 92,000,000 individuals may have been impacted in the Data Breach.

53. Plaintiff's claims are typical of the claims of the Class Members, since all such claims arise out of Defendants' failure to safeguard users' information.

54. Plaintiff does not have interests antagonistic to the interests of the Class.

55. The Class, of which Plaintiff is a member, is readily identifiable by reference to Defendants' records.

56. Plaintiff will fairly and adequately protect the interests of the Class and has retained competent counsel experienced in the prosecution of consumer litigation. Proposed Class Counsel has investigated and identified potential claims in the action; has a great deal of experience in handling class actions, other complex litigation, and claims of the type asserted in this action.

57. There are common questions of law and fact affecting the rights of all Class Members, including the following:

a. Whether Defendants violated Utah law by failing to implement reasonable security measures;

b. Whether Defendants violated common and statutory law by failing to promptly notify Class Members their Private Health Information and Personal Identifying Information had been compromised;

c. Whether class members may obtain injunctive relief against Defendants under Utah law to require that Defendants safeguard or destroy, rather than retain as it has, the Private Health Information and Personal Identifying Information of Plaintiff and Class Members;

d. Whether Defendants continue to use inadequate security measures to secure Plaintiff's and Class Members' Private Health Information and Personal Health Information;

e. Whether Plaintiff and Class Members are entitled to injunctive relief requiring Defendants to improve the security measures utilized to secure Private Health Information and Personal Identifying Information;

f. Which security procedures and which data breach notification procedure Defendants should be required to implement as part of any injunctive relief the Court orders;

g. Whether Defendants have contractual obligations to use reasonable security measures;

h. Whether Defendants have complied with contractual obligations to use reasonable security measures;

i. What security measures, if any, Defendants must implement to comply with their contractual obligations;

j. Whether Defendants have implied contractual obligations to use reasonable security measures;

k. Whether Defendants have complied with implied contractual obligations to use reasonable security measures;

l. What security measures, if any, Defendants must implement to comply with their implied contractual obligations;

m. Whether Defendants violated Utah privacy laws in connection with the actions described herein; and

n. What the nature of the relief should be, including equitable relief, to which Plaintiff and Class Members are entitled.

58. A class action is superior to other available methods for the fair and efficient adjudication of this controversy since joinder of all members is impracticable. While the economic damages suffered by the individual Class Members are significant, the amount is modest compared to the expense and burden of individual litigation. A class action will cause an orderly and expeditious administration of the claims of the Class and will foster economies of time, effort and expense.

59. The questions of law and/or fact common to the Class Members predominate over any questions affecting only individual members.

60. The prosecution of separate actions by individual Class Members would run the risk of inconsistent or varying adjudications, which would establish incompatible standards of conduct for the Defendants in this action or the prosecution of separate actions by individual Class Members would create the risk that adjudications with respect to individual Class Members would, as a practical matter, be dispositive of the interests of the other members not parties to the adjudications or substantially impair or impede their ability to protect their interests. Prosecution as a class action will eliminate the possibility of repetitious litigation.

61. Defendants have acted or refused to act on grounds generally applicable to the Class, thereby making appropriate final injunctive relief or corresponding declaratory relief with respect to the class as a whole.

62. Plaintiff does not anticipate any difficulty in the management of this litigation.

COUNT ONE

Negligence
(On Behalf of Plaintiff and the Class)

63. Plaintiff repeats and realleges the allegations set forth in paragraphs 1 through 50, as if fully set forth herein.

64. Defendants, through the course of providing services to Plaintiff and the Class, obtained their Private Information.

65. Defendants knew, or should have known, of the risks inherent in collecting and storing the Private Information of Plaintiff and Class Members.

66. Upon accepting and storing Plaintiff's and Class Members' Private Information in their computer database systems, Defendants undertook and owed a duty to Plaintiff and Class Members to exercise reasonable care to secure and safeguard that information and to utilize commercially reasonable methods to do so. Defendants knew, acknowledged, and agreed

Plaintiff's and Class Members' Private Information was private and confidential, and should be protected as private and confidential.

67. The breach of confidentiality for DNA genealogy results was a breach of the standard of care owed by Defendants to Plaintiff and Class Members.

68. Defendants breached their duties of care to Plaintiff and Class Members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Private Information.

69. Defendants acted with wanton disregard for the security of Plaintiff's and Class Members' Private Information. Defendants knew or should have known they had inadequate computer systems and data security practices to safeguard such information, and Defendants knew or should have known that hackers were attempting to access the PHI and PII in DNA databases such as Defendants'.

70. The law imposes an affirmative duty on Defendants to timely discover and disclose the unauthorized access and theft of Plaintiff's and Class Members' Private Information so that Plaintiff and Class Members could take appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuse of their Private Information.

71. To date, Defendants have not provided sufficient information to Plaintiff and Class Members regarding the extent of the unauthorized access, and continue to breach their disclosure obligations to Plaintiff and Class Members.

72. Defendants have not notified the Class of what DNA information was disclosed, and specifically what Private Information was disclosed for each Class Member in the breach.

73. Furthermore, Defendants' notification letter was misleading in that it represented that Defendants had fixed the flaw, which permitted the breach, when in reality Defendants do not know how the breach occurred.

74. Defendants also breached their duty to Plaintiff and Class Members to adequately protect and safeguard Plaintiff's and Class Members' Private Information by knowingly disregarding standard information security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to unsecured Private Information. Furthering their dilatory practices, Defendants failed to provide adequate supervision and oversight of the Private Information with which they were entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted a third party to gather Plaintiff's and Class Members' Private Information, misuse the Private Information, and intentionally disclose it to others without consent.

75. Through Defendants' acts and omissions described in this Complaint, including Defendants' failure to provide adequate security and their failure to protect Plaintiff's and Class Members' Private Information from being foreseeably captured, accessed, disseminated, stolen, and misused, Defendants unlawfully breached their collective duty to use reasonable care to adequately protect and secure Plaintiff's and Class Members' Private Information during the time it was within Defendants' possession or control.

76. Further, through their failure to timely discover and provide clear notification of the Data Breach to consumers, Defendants prevented Plaintiff and Class Members from taking meaningful, proactive steps to secure their Private Information.

77. Upon information and belief, Defendants improperly and inadequately safeguarded the Private Information of Plaintiff and Class Members in deviation from standard industry rules, regulations, and practices at the time of the Data Breach.

78. Defendants' failure to take proper security measures to protect Plaintiff's and Class Members' sensitive Private Information as described in this Complaint, created conditions conducive to a foreseeable, intentional criminal act, namely the unauthorized access of Plaintiff's and Class Members' Private Information.

79. Defendants' conduct was grossly negligent and departed from all reasonable standards of care, including, but not limited to: failing to adequately protect the Private Information; failing to conduct adequate, regular security audits; failing to provide adequate and appropriate supervision of persons having access to Plaintiff's and Class Members' Private Information; and failing to provide Plaintiff and Class Members with timely and sufficient notice that their sensitive Private Information had been compromised.

80. Neither Plaintiff nor the Class Members contributed to the Data Breach and subsequent misuse of their Private Information as described in this Complaint.

81. As a direct and proximate cause of Defendants' conduct, Plaintiff and Class Members suffered damages including, but not limited to: damages from identity theft, which may take months, if not years, to discover and detect, given the far-reaching, adverse, and detrimental consequences of identity theft and loss of privacy; as well as damages related to the unauthorized dissemination of Plaintiff's and Class Members' genealogy. The nature of other forms of economic damage and injury may take years to detect and the potential scope can only be assessed after a thorough investigation of the facts and events surrounding the theft mentioned above.

COUNT TWO

Breach of Contract
(On Behalf of Plaintiff and the Class)

82. Plaintiff repeats and realleges the allegations set forth in paragraphs 1 through 50, as if fully set forth herein.

83. As set forth above, Plaintiff and Class Members received services from Defendants, including family histories, DNA genealogy, and other ancestry products.

84. As set forth above, the contract between Plaintiff and Class Members and Defendants was supported by consideration in many forms including the payment of monies for DNA testing services, and/or the enrollment in Defendants' services, which permitted Defendants to market the vast user network and refine their testing procedures to produce more accurate results as the user base increases.

85. Plaintiff and Class Members performed pursuant to these contracts, and satisfied all conditions, covenants, obligations, and promises of the agreements.

86. Under the contracts, Defendants were obligated, as outlined in the Privacy Policy, to maintain the confidentiality of Plaintiff's and Class Members' Private Information.

87. Defendants' failure to maintain the confidentiality of Plaintiff's and Class Members' Private Health Information was a breach of Defendants' contractual obligations as outlined in the Privacy Policy.

88. Defendants' failure to maintain the confidentiality of Plaintiff's and Class Members' Personal Identifying Information was a breach of Defendants' contractual obligations as outlined in the Privacy Policy.

89. As a result of Defendants' breach of contract, by failing to adequately secure Plaintiff's and Class Members' PHI and PII, Plaintiff and Class Members did not receive the full

benefit of the bargain, and instead received services that were less valuable than described in the contracts. Plaintiff and Class Members, therefore, were damaged in an amount at least equal to the difference in value between what was promised and what Defendants ultimately provided.

90. Also as a result of Defendants' breach of contract, Plaintiff and Class Members have suffered actual damages resulting from the theft of their PHI and PII, and remain at imminent risk of suffering additional breaches in the future.

COUNT THREE

Breach of Implied Contract
(On Behalf of Plaintiff and the Class)

91. Plaintiff repeats and realleges the allegations set forth in paragraphs 1 through 50, as if fully set forth herein.

92. Defendants solicited and invited Plaintiff and Class Members to use their services. Plaintiff and Class Members accepted Defendants' offers and created user accounts requiring the provision of PHI and PII with Defendants.

93. When Plaintiff and Class Members used Defendants' services and products, they provided their PHI and PII. In so doing, Plaintiff and Class Members entered into implied contracts with Defendants pursuant to which Defendants agreed to safeguard and protect such information and to timely and accurately notify Plaintiff and Class Members if their data had been breached and compromised.

94. Each use of Defendants' services or products by Plaintiff and Class Members was made pursuant to the mutually agreed-upon implied contracts with Defendants under which Defendants agreed to safeguard and protect Plaintiff's and Class Members' PHI and PII, and to timely and accurately notify them if and when such information was compromised or stolen.

95. Plaintiff and Class Members would not have provided and entrusted their PHI and PII to Defendants in the absence of the implied contracts.

96. Plaintiff and Class Members fully performed their obligations under the implied contracts with Defendants.

97. Defendants breached the implied contracts they made with Plaintiff and Class Members by failing to safeguard and protect Plaintiff's and Class Members' PHI and PII, and by failing to provide timely and accurate notice to them that their PHI and PII was compromised in and as a result of the Data Breach.

98. As a direct and proximate result of Defendants' breaches of the implied contracts, Plaintiff and Class Members sustained actual losses and damages as described in detail above.

COUNT FOUR

Invasion of Privacy
(On Behalf of Plaintiff and the Class)

99. Plaintiff repeats and realleges the allegations set forth in paragraphs 1 through 50, as if fully set forth herein.

100. Plaintiff's and Class Members' PII and PHI is private information.

101. Dissemination and publication of Plaintiff's and Class Members' PII and PHI would be offensive to a reasonable person.

102. The public has no legitimate interest in being apprised of Plaintiff's and Class Members' PII and PHI.

103. Defendants' failure to safeguard and protect Plaintiff's and Class Members' PII and PHI directly and proximately resulted in unreasonable publicity of Plaintiff's and Class Members' private lives.

104. Plaintiff and Class Members have a legal interest in the privacy of their PII and

PHI.

105. Defendants' failure to safeguard and protect Plaintiff's and Class Members' PII and PHI was a direct and proximate cause of an unauthorized third party accessing and obtaining Plaintiff's and Class Members' PII and PHI as a matter of law.

106. Defendants' failure to safeguard and protect Plaintiff's and Class Members' PII and PHI deprived Plaintiff and Class Members of their legal interest in the privacy of that information, causing them damages.

107. As a result of Defendants' actions and inactions resulting in Plaintiff's and Class Members' loss of privacy, Plaintiff and Class Members were and continue to be injured and have suffered damages.

COUNT FIVE

Publication of Private Facts
(On Behalf of Plaintiff and the Class)

108. Plaintiff repeats and realleges the allegations set forth in paragraphs 1 through 50, as if fully set forth herein.

109. Defendants, by and through their failure to adequately safeguard Plaintiff's and Class Members' PHI and PII, have made Plaintiff's and Class Members' information public.

110. Plaintiff's and Class Members' private medical results, lists of treating doctors and other sensitive information were private, as Defendant acknowledged as aforesaid.

111. Dissemination of information such as the PHI and PII revealed by Defendant about Plaintiff and Class Members would be offensive to a reasonable person.

112. Plaintiff's and other Class Members' PHI and PII is not of legitimate public concern, and there is no legitimate public interest in the public being apprised of said information.

113. Plaintiff and other Class Members did not consent to the disclosure of their PHI and PII.

114. As a direct and proximate result of Defendants' breaches of the implied contracts between Defendants and Plaintiff (and Class Members), Plaintiff and Class Members sustained actual losses and damages as described in detail above. Additionally Plaintiff and Class members are entitled to presumed damages as a result of Defendants' publication of private facts.

COUNT SIX

Unjust Enrichment
(On Behalf of Plaintiff and the Class)

115. Plaintiff repeats and realleges the allegations set forth in paragraphs 1 through 50, as if fully set forth herein.

116. In the alternative to the above plead claims, Plaintiff and Class Members allege they have no adequate remedy at law and bring this unjust enrichment claim.

117. Plaintiff and Class Members conferred a monetary benefit on Defendants, by their participation in Defendants' services and products, which Defendants used to market the vast user network and refine their testing procedures to produce more accurate results as the user base increases.

118. Defendants appreciated or had knowledge of the benefits conferred upon them by Plaintiff and Class Members.

119. The amounts paid to Defendants (partially) as a result of Plaintiff's and Class Members' participation in Defendants' services and products should have been used by Defendants in part to pay for the administrative costs of reasonable data privacy and security practices and procedures.

120. As a result of Defendants' conduct, Plaintiff and Class Members suffered actual damages as aforesaid.

121. Under principals of equity, Defendants should not be permitted to retain the money they collected as a result of Plaintiff's and Class Members' participation in Defendants' services and products because Defendants failed to implement (or adequately implement) the data privacy and security practices and procedures to which Plaintiff and Class Members were fairly entitled, and which were otherwise mandated by HIPAA regulations, federal, state and local laws, as well as industry standards.

122. Defendants should be compelled to disgorge into a common fund for the benefit of Plaintiff and Class Members all unlawful or inequitable proceeds received.

COUNT SEVEN

Violation of the Utah Consumer Sales Practices Act
Utah Code 13-11-1, *et seq.*
(On Behalf of Plaintiff and the Class)

123. Plaintiff repeats and realleges the allegations set forth in paragraphs 1 through 50, as if fully set forth herein.

124. Plaintiff and Class Members bring these claims against Defendants under the Utah Consumer Sales Practices Act.

125. Plaintiff and Class Members are "persons" under the Utah Consumer Sales Practices Act.

126. Defendants are "suppliers" under the Utah Consumer Sales Practices Act.

127. Defendant engages in "consumer transactions" as defined by the Utah Consumer Sales Practices Act by selling, leasing, assigning, transferring, or otherwise disposing of goods, services, or other property for primarily personal, family, or household purposes.

128. Defendant engaged in unconscionable and deceptive acts and practices, misrepresentation and the concealment, suppression, and omission of material facts with respect to the consumer transactions of their services in violation of the Utah Consumer Sales Practices Act, including by not limited to the following:

a. Misrepresenting material facts, pertaining to their services to consumers by representing that they would maintain adequate data privacy and security practices and procedures to safeguard Plaintiff's and Class Members' PHI and PII from unauthorized disclosure, release, data breaches, and theft;

b. Misrepresenting material facts by representing to Plaintiff and Class Members that they did and would continue to comply with the relevant industry data security standards, state law, and federal law with regard to the protection of Plaintiff's and Class Members' PHI and PII;

c. Defendants knowingly omitted, suppressed, and concealed the material fact of the inadequacy of the privacy and security protections for Plaintiff's and Class Members' PHI and PII with the intent that Plaintiff and Class Members would rely on the omission, suppression, and concealment; and

d. Defendant engaged in unconscionable and deceptive acts and practices by failing to disclose the Data Breach to Plaintiff and Class Members in a timely and accurate manner.

129. As a direct and proximate result of Defendants' unconscionable or deceptive acts and practices, Plaintiff and Class Members suffered an ascertainable loss in moneys or property,

real or personal, as described above, including the loss of their legally protected interest in the confidentiality and privacy of their PHI and PII.

130. Plaintiff and Class members are therefore entitled to injunctive relief, equitable relief, actual damages, and attorneys' fees and costs pursuant to Utah Code 13-11-19(3)–(5).

COUNT EIGHT

Declaratory and Injunctive Relief

(On Behalf of Plaintiff and the Class)

131. Plaintiff repeats and realleges the allegations set forth in paragraphs 1 through 50, as if fully set forth herein.

132. Under the Declaratory Judgment Act, 28 U.S.C. § 2201 *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, which are tortious and which violate the terms of the statutes described in this complaint.

133. An actual controversy has arisen in the wake of Defendants' Data Breach regarding their common law and other duties to reasonably safeguard their customers' Private Health Information and Personal Identifying Information. Plaintiff alleges Defendants' data security measures were inadequate and remain inadequate. Plaintiff continues to suffer injury as her Private Information is inadequately secured.

134. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendants owed and continue to owe a legal duty to secure their customers' personal and financial information—specifically including information pertaining to Private Health Information and DNA genealogy information;

b. Defendants breached and continue to breach this legal duty by failing to employ reasonable measures to secure their customers' Private Health Information.

c. Defendants' breach of their legal duty proximately caused the Data Breach which Defendants announced on or about June 4, 2018; and

d. Defendants have been unable to identify the flaw in their security, which allowed the Data Breach to occur and has therefore, not fixed said flaw, meaning customers' Private Information continues to be insecure.

135. The Court also should issue corresponding injunctive relief requiring Defendants to employ adequate security protocols to protect their customers' Private Information, specifically, this injunction should, among other things, direct Defendants to:

a. Identify the security flaw which permitted the Data Breach;

b. Implement adequate security measures to fix the security flaw which permitted the Data Breach on October 26, 2017;

c. Engage third party auditors to test their systems for weakness and upgrade any such weakness found;

d. Audit, test, and train their data security personnel regarding any new or modified procedures and how to respond to a data breach;

e. Regularly test their systems for security vulnerabilities, consistent with industry standards;

f. Advise customers of which DNA genealogy results and what Private Information was disclosed in the Data Breach;

136. If an injunction is not issued, Plaintiff and Class Members will suffer irreparable injury and lack an adequate legal remedy in the event of another data breach at Defendants'. The risk of another such breach is real, immediate, and substantial. If another breach at Defendants occurs, Plaintiff and Class Members will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

137. The hardship to Plaintiff and absent Class Members if an injunction does not issue exceeds the hardship to Defendants if an injunction is issued. Among other things, if another data breach occurs at Defendants, Plaintiff and the absent Class Members will likely incur significant additional harm in the loss of privacy and publication of their Private Information. On the other hand, the cost to Defendants of complying with an injunction by employing reasonable data security measures is relatively minimal and Defendants have pre-existing legal obligations to employ such measures.

138. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at Defendants, thus eliminating the injuries that would result to Plaintiff and the numerous other consumers whose confidential information would be compromised.

REQUEST FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all Class Members proposed in this Complaint, respectfully requests that the Court enter judgment in her favor and against Defendants as follows:

a. For an Order certifying the Class as defined here, and appointing Plaintiff and her Counsel to represent the Class;

b. For equitable relief enjoining Defendants from engaging in the wrongful conduct complained of here pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' Private Health Information and Personal Identifying Information, and from refusing to issue prompt, complete, and accurate disclosures to Plaintiff and Class Members;

c. For equitable relief compelling Defendants to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety and to disclose with specificity to Class Members the type of Private Health Information and Personal Identifying Information compromised.

d. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendants' wrongful conduct;

e. For an award of actual damages and compensatory damages, in an amount to be determined;

f. For an award of treble damages, as allowable by law;

g. For an award of costs of suit and attorneys' fees, as allowable by law; and

h. Such other and further relief as this court may deem just and proper.

DATED: September 12, 2018.

/s/ Steven A. Christensen

Steven A. Christensen
9980 S. 300 W. Ste. 200
Sandy, Utah 84070
Tel: (801) 676-6447
Email: steven@christensenyounglaw.com

JURY TRIAL DEMAND

Pursuant to Rule 38 of the Federal Rules of Civil Procedure, Plaintiff demands a jury trial on all issues so triable.

DATED: September 12, 2018.

/s/ Steven A. Christensen
Steven A. Christensen
9980 S. 300 W. Ste. 200
Sandy, Utah 84070
Tel: (801) 676-6447
Email: steven@christensenyounglaw.com

Attorneys for Plaintiff and the Putative Class

JS 44 (Rev. 08/18)

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 Hall, Showneen

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

(c) Attorneys *(Firm Name, Address, and Telephone Number)*
Christensen Young & Associates, PLLC
9980 So. 300 West, #200, Sandy, UT 84070 (801) 676-6447

DEFENDANTS MyHeritage, Ltd.
MyHeritage (USA), Inc.

County of Residence of First Listed Defendant Utah
(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
- ☐ 485 Telephone Consumer Protection Act
- ☐ 490 Cable/Sat TV
- ☐ 850 Securities/Commodities/ Exchange
- ☐ 890 Other Statutory Actions
- ☐ 891 Agricultural Acts
- ☐ 893 Environmental Matters
- ☐ 895 Freedom of Information Act
- ☐ 896 Arbitration
- ☐ 899 Administrative Procedure Act/Review or Appeal of Agency Decision
- ☐ 950 Constitutionality of State Statutes

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

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

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing *(Do not cite jurisdictional statutes unless diversity)*:
28 USC 1332 (d), 28 USC 1367

Brief description of cause:
Data breach

VII. REQUESTED IN COMPLAINT:

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

DEMAND $

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

VIII. RELATED CASE(S) IF ANY *(See instructions)*:

JUDGE _____ DOCKET NUMBER _____

DATE
09/12/2018

SIGNATURE OF ATTORNEY OF RECORD
/s/ Steven A. Christensen

FOR OFFICE USE ONLY

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