**IN THE UNITED STATES DISTRICT COURT**
**FOR THE NORTHERN DISTRICT OF ILLINOIS**

| | |
|---|---|
| ALYSON HU, individually and on behalf of all others similarly situated,<br><br>Plaintiff,<br><br>v.<br><br>23ANDME, INC.,<br><br>Defendant. | Case No.: 1:23-cv-17079<br><br>**CLASS ACTION COMPLAINT**<br><br>**DEMAND FOR JURY TRIAL** |

Plaintiff Alyson Hu ("Plaintiff"), by her undersigned counsel, files this Class Action Complaint, individually and on behalf a class of all similarly situated persons, against Defendant 23andMe, Inc. ("Defendant" or "23andMe"). Plaintiff bases the following allegations on personal knowledge, due investigation of counsel, and, where indicated, on information and belief, and states the following:

## NATURE OF THE ACTION

1. 23andMe is a popular personal genomics and biotechnology company that uses direct-to-consumer genetic testing to create unique, personalized genetic reports on genetic ancestral origins, personal genetic health risks, chances of passing on carrier conditions, and pharmacogenetics.[1] 23andMe pitches itself "as [one of the] guardians of our genetic history, as [a] gatekeeper[] of our ancestral pasts and potential medical futures."[2] But despite 23andMe

[1] 23andMe Holding Co., Form 10-K, U.S. Sec. Exch. Comm'n (March 31, 2023), https://www.sec.gov/ix?doc=/Archives/edgar/data/1804591/000095017023024232/me-20230331.htm (last accessed Dec. 26, 2023).

[2] Haje Jan Kamps, *DNA companies should receive the death penalty for getting hacked*, TechCrunch (Dec. 8, 2023), DNA companies should receive the death penalty for getting hacked | TechCrunch (last accessed Dec. 26, 2023).

considering itself as a gatekeeper of our sensitive genetic history, Defendant instead failed to safeguard the sensitive, personal information it was entrusted. And when that information was stolen by cybercriminals and offered for sale on the dark web, 23andMe decided to "hide behind the old 'we were not hacked; it was the users' old passwords' excuse."[3]

2. As a provider of genetic testing, 23andMe understood it had the duty and responsibility to protect patients' information that it collected, stored, and maintained, expressly advertising to potential customers that "at 23andMe, Privacy is in our DNA."[4] Defendant failed to meet its duty and, as a direct result, the sensitive customer information with which it was entrusted was released, stolen, and offered for sale on the dark web.

3. On October 6, 2023, in a blog post on its website, Defendant announced that unauthorized threat actors had accessed 23andMe.com accounts without authorization and compiled exfiltrated customers' information, including information derived from genetic testing (the "Data Breach").[5]

4. The sensitive personally identifying information ("PII") released to the threat actors included millions of individuals' information derived from genetic testing, and including, *inter alia*, records identifying names, usernames, regional locations, profile photos, birth years, and data about individuals' ethnicities.

5. In order to obtain Defendant's services, individuals must entrust 23andMe with sensitive, private information. Defendant requires this information in order to perform its regular

---

[3] *Id.*

[4] *Privacy Statement*, 23andMe (updated Oct. 4, 2023) https://www.23andme.com/legal/privacy/full-version/ (last accessed Dec. 26, 2023).

[5] Addressing Data Security Concerns ("Notice"), 23andMe (Oct. 6, 2023), https://blog.23andme.com/articles/addressing-data-security-concerns (last updated Dec. 5, 2023) (last accessed Dec. 26, 2023).

business activities. Additionally, the reports generated by Defendant contain sensitive, private information derived from genetic testing.

6. Since the Data Breach occurred, several news sources have reported that threat actors listed mass amounts of the stolen data for sale on the dark web.[6] Defendant has failed to address these reports, failed to inform victims when and how the Data Breach occurred, and has even failed to say whether the security threat is still a risk to its customers.

7. As a result of Defendant's failure to implement adequate data security measures, Plaintiff and Class Members have suffered actual harm in the form of misuse of their PII and are subject to increased risk of harm due to the exposure and publishing of their PII on the dark web, including the certainly impending and increased risk of identity theft. As such, Plaintiff and Class Members assert claims for negligence and for violations of the Illinois Genetic Information Privacy Act ("GIPA"), 410 ILCS 513/1, *et seq*.

## JURISDICTION AND VENUE

8. This Court has jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2) because Plaintiff and at least one member of the Class, as defined below, is a citizen of a different state than Defendant, there are more than 100 putative class members, and the amount in controversy exceeds $5 million exclusive of interest and costs.

9. This Court has personal jurisdiction over Defendant because Defendant regularly conducts business in Illinois, and has sufficient minimum contacts with Illinois because they conduct substantial business in the State of Illinois.

---

[6] Joseph Menn, *Genetic Tester 23andMe's Hacked Data on Jewish Users Offered for Sale Online*, Wash. Post (Oct. 6, 2023), https://www.washingtonpost.com/technology/2023/10/06/23andme-hacked-data/; Steve Adler, *23andMe User Data Stolen in Credential Stuffing Attack*, HIPAA Journal (Oct. 10, 2023), https://www.hipaajournal.com/23andme-user-data-stolen-credential-stuffing-campaign/ (last accessed Dec. 26, 2023).

10. This Court is the proper venue for this case pursuant to 28 U.S.C. § 1391 because a substantial part of the events and omissions giving rise to Plaintiff's claims occurred in Illinois, Defendant conducts substantial business within this District, and Defendant has harmed Class Members residing in this District.

## PARTIES

11. Plaintiff Alyson Hu is an adult, who at all relevant times, is and was a citizen and resident of the State of Illinois. Plaintiff is a customer of 23andMe who received a notice from Defendant, informing her that her PII provided to Defendant had been compromised in the Data breach.

12. Defendant 23andMe, Inc., is a Delaware corporation that maintains its headquarters at 223 N. Mathilda Ave., Sunnyvale, CA 94086.

## FACTUAL BACKGROUND

### *A. Defendant Provides Technology Services Involving Highly Sensitive Data.*

13. 23andMe is a personal genomics and biotechnology company with reported annual earnings of $299 million and a customer base of "over 14 million genotyped customers" on what it calls "the world's largest, re-contactable crowdsourced platform of genotypic information."[7]

14. 23andMe uses direct-to-consumer genetic testing to create detailed, individualized genetic reports, including information such as: ancestry composition and detail, maternal and paternal haplogroups, DNA relatives, genetic health predispositions, carrier status, genetic traits, wellness, and pharmacogenetics (*i.e.*, how a person's genes affect medication response).[8]

[7] *23andMe Reports FY2023 Fourth Quarter and Full Year Financial Results*, 23andMe (May 25, 2023), https://investors.23andme.com/news-releases/news-release-details/23andme-reports-fy2023-fourth-quarter-and-full-year-financial (last accessed Dec. 26, 2023).
[8] *How it Works*, 23andMe, https://www.23andme.com/howitworks/, (last accessed Dec. 26, 2023).

15. As a condition of receiving 23andMe's services, customers must provide it with sensitive PII, including highly sensitive information derived from genetic testing. On its website, 23andMe lists the PII that it collects, including, but not limited to, the following types of information:

a. Registration information, such as name, user ID, password, date of birth, billing address, shipping address, payment information (*e.g.*, credit card), account authentication information, and contact information (*e.g.*, email, phone number);

b. Genetic information, including information regarding genotype, genetic data, and generated reports with findings based on genetic information;

c. Saliva sample information regarding the sample submitted for genetic testing and analysis, laboratory values, and other data provided through 23andMe's services; and

d. Self-reported information, such as gender, disease conditions, health-related information, traits, ethnicity, and family history.[9]

16. 23andMe derives substantial benefit from this information because Defendant profits from the sale of its genetic testing kits and, but for the collection of Plaintiff's and Class Members' PII, Defendant would be unable to perform its various services.

17. 23andMe acknowledges the vast amounts of PII with which it is entrusted and claims, "At 23andMe, Privacy is in our DNA."[10]

[9] *Privacy Statement*, 23andMe, https://www.23andme.com/legal/privacy/full-version/ (updated Oct. 4, 2023) (last accessed Dec. 26, 2023).
[10] *Id.*

18. 23andMe goes so far as to boldly promise its customers: "The only way your data would be shared with third parties would be by your choice."[11]

19. Plaintiff and Class Members had a reasonable expectation based on Defendant's statements that their sensitive personal information would be protected. However, despite 23andMe's purported commitment to data security, Defendant failed to prioritize data protection and cybersecurity of its customers' PII by adopting reasonable data and cybersecurity measures to prevent the unauthorized access to Plaintiff's and Class Members' PII and allowed for the release of said information to unauthorized bad actors where it was subsequently posted for sale on the dark web.

***B. The Data Breach was a Foreseeable Risk of which Defendant was on Notice.***

20. 23andMe was well aware that the PII it acquires is highly sensitive and of significant value to those who would use it for wrongful purposes.

21. 23andMe also knew that a breach of its computer systems, and release of the information stored therein, would result in the increased risk of identity theft and fraud against the individuals whose PII was compromised, as well as intrusion into their highly private information.

22. These risks are not theoretical, there have been numerous high profile data breaches at other genetic testing companies, including DNA Diagnostics Center, Ambry Genetics, and MyHeritage.

23. PII, including genetic information, is a valuable commodity to identity thieves. As the FTC recognizes, identity thieves can use this information to commit an array of crimes

[11] *How Will You Safeguard My Information?*, 23andMe, https://customercare.23andme.com/hc/en-us/articles/202907850-How-Will-You-Safeguard-My-Information- (last accessed Dec. 26, 2023).

including identity theft, and medical and financial fraud.[12] Indeed, a robust "cyber black market" exists in which criminals openly post stolen PII and other protected financial information on multiple underground Internet websites, commonly referred to as the "dark web."

24. Criminals often trade stolen PII on the "cyber black market" for years following a breach. Cybercriminals can also post stolen PII on the internet, thereby making such information publicly available. Indeed, the information compromised during the Data Breach is already being offered for sale on the Dark Web, with an advertisement claiming that the stolen PII is "the most valuable data you'll ever see."[13]

25. The prevalence of data breaches and identity theft has increased dramatically in recent years, accompanied by a parallel and growing economic drain on individuals, businesses, and government entities in the U.S. In 2021, there were 4,145 publicly disclosed data breaches, exposing 22 billion records. The United States specifically saw a 10% increase in the total number of data breaches.[14]

26. In tandem with the increase in data breaches, the rate of identity theft complaints has also increased over the past few years. For instance, in 2017, 2.9 million people reported some form of identity fraud compared to 5.7 million people in 2021.[15]

---

[12] *What To Know About Identity Theft*, Fed. Trade Comm'n Consumer Advice (Apr. 2021), https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft (last accessed Dec. 26, 2023).

[13] Dark Reading Staff, *23andMe Cyberbreach Exposes DNA Data, Potential Family Ties*, DarkReading (Oct. 6, 2023), https://www.darkreading.com/cyberattacks-data-breaches/23andme-cyberbreach-exposed-dna-data-family-ties (last accessed Dec. 26, 2023).

[14] *Data Breach Report: 2021 Year End*, Risk Based Security (Feb. 4, 2022), https://www.riskbasedsecurity.com/2022/02/04/data-breach-report-2021-year-end/ (last accessed Dec. 26, 2023).

[15] *Insurance Information Institute, Facts + Statistics: Identity theft and cybercrime*, Insurance Information Institute, https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime#Identity%20Theft%20And%20Fraud%20Reports,%202015-2019%20 (last accessed Dec. 26, 2023).

27. Cybercriminals target genetic testing companies because they are "treasure troves" of sensitive information. Some sites offer users the option to download a copy of their full genetic code while others don't. "But the full genetic code isn't the most valuable information anyway. . . [W]e can't just read genetic code like a book to gain insights. Instead, it's the easy-to-access account pages with health interpretations that are most useful for hackers."[16]

28. The breath of data compromised makes the information particularly vulnerable to thieves and leaves 23andMe's customers especially vulnerable to fraud and other risks.

29. Genetic testing information is extremely valuable to cybercriminals because it can be sold or monetized to insurance companies to calculate the costs of health insurance and life insurance. And, in addition to insurance companies, there are numerous other entities that want DNA, including researchers who want genetic information for scientific studies; police departments who want genetic information to catch criminals; individuals who want to use it to genetically discriminate against people, including denying mortgages or increasing insurance costs; or by other cybercriminals who can use the information for blackmail. As one professor has explained: "[i]f there is data that exists, there is a way for it to be exploited."[17]

30. The ramifications of 23andMe's failure to keep Plaintiff and Class Members' PII secure are long-lasting and severe. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.

[16] Angela Chen, *Why a DNA data breach is much worse than a credit card leak*, The Verge (Jun. 6, 2018), https://www.theverge.com/2018/6/6/17435166/myheritage-dna-breach-genetic-privacy-bioethics (last accessed Dec. 26, 2023).
[17] *Id.*

31. A data breach increases the risk of becoming a victim of identity theft. Victims of identity theft can suffer from both direct and indirect financial losses. According to a research study published by the Department of Justice:

> A direct financial loss is the monetary amount the offender obtained from misusing the victim's account or personal information, including the estimated value of goods, services, or cash obtained. It includes both out-of-pocket loss and any losses that were reimbursed to the victim. An indirect loss includes any other monetary cost caused by the identity theft, such as legal fees, bounced checks, and other miscellaneous expenses that are not reimbursed (e.g., postage, phone calls, or notary fees). All indirect losses are included in the calculation of out-of-pocket loss.[18]

32. Even if stolen PII does not include financial or payment card account information, that does not mean there has been no harm, or that the breach does not cause a substantial risk of identity theft. Freshly stolen information can be used with success against victims in specifically targeted efforts to commit identity theft known as social engineering or spear phishing. In these forms of attack, the criminal uses the previously obtained PII about the individual, such as name, address, email address, and affiliations, to gain trust and increase the likelihood that a victim will be deceived into providing the criminal with additional information.

33. A poll of security executives predicted an increase in attacks over the next two years from "social engineering and ransomware" as nation-states and cybercriminals grow more sophisticated. Unfortunately, these preventable causes will largely come from "misconfigurations, human error, poor maintenance, and unknown assets."[19]

---

[18] Erika Harrell, Bureau of Just. Stat., U.S. Dep't of Just., NCJ 256085, *Victims of Identity Theft*, 2018 I (2020) https://bjs.ojp.gov/content/pub/pdf/vit18.pdf (last accessed Dec. 26, 2023).
[19] Chuck Brooks, *Alarming Cyber Statistics For Mid-Year 2022 That You Need to Know*, Forbes (June 3, 2022), https://www.forbes.com/sites/chuckbrooks/2022/06/03/alarming-cyber-statistics-for-mid-year-2022-that-you-need-to-know/?sh=176bb6887864 (last accessed Dec. 26, 2023).

34. In light of high-profile data breaches at other companies, 23andMe knew or should have known that its computer systems would be targeted by cybercriminals.

35. Defendant also knew or should have known, the importance of safeguarding the PII with which it was entrusted and of the foreseeable consequences if its data security systems were breached. Defendant failed, however, to take adequate cybersecurity measures to prevent the Data Breach and release of its customers PII from occurring.

### *C. Defendant Released Highly Sensitive PII to Hackers.*

36. On October 6, 2023, 23andMe posted a notice ("Notice") on its website regarding the Data Breach in a blog post euphemistically titled "Addressing Data Security Concerns."[20]

37. The Notice reports that customer profile information shared through 23andMe's DNA Relatives feature was compiled by threat actors from individual accounts without account users' authorization.[21] The compromised DNA Relatives feature includes, *inter alia*, customers' display names, genetic ancestry, familial connections, location, and profile pictures.[22]

38. 23andMe's DNA Relatives feature is an optional feature that allows Defendant's customers to find and connect with their genetic relatives by comparing the DNA they provided to Defendant with the DNA that other customers have provided to Defendant.

39. The language of the Notice seems to place the blame on Defendant's customers, asserting that the Data Breach was caused by and affected individuals who "recycled login credentials" and opted-in to the DNA Relatives feature.[23] But that is not the case. The Data Breach

---

[20] Notice, *supra* note 5.
[21] *Id.*
[22] *DNA Relatives Privacy & Display Settings*, 23andMe, https://customercare.23andme.com/hc/en-us/articles/212170838-DNA-Relatives-Privacy-Display-Settings (last accessed Dec. 26, 2023).
[23] Lorenzo Franceschi-Bicchierai, *23andMe confirms hackers stole ancestry data on 6.9 million users*, TechCrunch (Dec. 5, 2023), https://techcrunch.com/2023/12/04/23andme-confirms-hackers-stole-ancestry-data-on-6-9-million-users/ (last accessed Dec. 26, 2023).

is the result of Defendant's failure to implement inadequate data security measures. Defendant has indicated that while the threat actor only accessed a limited number of accounts (a mere 14,000), the threat actor was nevertheless able to access the PII of approximately 6.9 million individuals through Defendant's DNA Relatives feature.[24] Put differently, customer information was released through 23andMe's DNA Relatives feature without authorization, exposing countless customers PII.

40. Notably, the Notice does not state when the Data Breach occurred, when 23andMe gained knowledge of the Data Breach (other than vaguely saying that 23andMe learned of the incident "recently"), or how many people were affected.[25] Defendant has not released this information to date.

41. Despite Defendant's limited statements about the incident, it has been widely investigated and covered in the press. Before Defendant announced the Data Breach, news reports indicated that a threat actor posted a link to a sample of stolen data on a popular dark web forum, which included 1 million lines of data for Ashkenazi people that belonged to 23andMe customers.[26] Soon after, the threat actor began offering to sell data profiles in bulk for $1-$10 depending on how many profiles were purchased.[27] 23andMe later confirmed the stolen data for sale was legitimate.[28]

42. Following the initial leak, news reports further reported that the threat actor responsible for the leaked information then later leaked millions more 23andMe user records.

---

[24] Notice, *supra* note 5.
[25] *Id.*
[26] Bill Toulas, *Genetics firm 23andMe say user data stolen in credential stuffing attack*, BleepingComputer (Oct. 6, 2023), https://www.bleepingcomputer.com/news/security/genetics-firm-23andme-says-user-data-stolen-in-credential-stuffing-attack/ (last accessed Dec. 26, 2023).
[27] *Id.*
[28] *Id.*

These news reports have confirmed that some of the leaked information matches known and public 23andMe user and genetic information.[29]

43. One report estimates that the Data Breach "could cover more than half of the company's 14 million customers" based on the number of people who opted-in to the DNA Relatives feature.[30]

44. Investigative journalists have also reported that the incident "appears to have been conducted, or at least launched, several months ago" based on a post in a cybercrime forum on the dark web from August 11, 2023, in which a hacker advertised a set of 23andMe user data that matched leaked user records.[31]

45. Accordingly, the Data Breach has resulted in not only the exfiltration of 23andMe customers' PII, but also in the sale of that PII on the dark web.

46. In sum, upon information and belief, as a result of Defendant's failure to implement adequate data security measures, Plaintiff's and Class Members' PII, including genetic information, was negligently released to unauthorized, malicious threat actors and is now at risk of dissemination and use by other unauthorized individuals or cybercrime groups.

***D. Defendant Failed to Comply with FTC Guidelines.***

47. 23andMe is prohibited by the Federal Trade Commission Act, 15 U.S.C. § 45 ("FTC Act") from engaging in "unfair or deceptive acts or practices in or affecting commerce."

---

[29] Lorenzo Franceschi-Bicchierai, *Hacker leaks millions more 23andMe user records on cybercrime forum*, TechCrunch (Oct. 18, 2023), https://techcrunch.com/2023/10/18/hacker-leaks-millions-more-23andme-user-records-on-cybercrime-forum/ (last accessed Dec. 26, 2023).

[30] Joseph Menn, *Genetic Tester 23andMe's Hacked Data on Jewish Users Offered for Sale Online*, Wash. Post (Oct. 6, 2023), https://www.washingtonpost.com/technology/2023/10/06/23andme-hacked-data/ (last accessed Dec. 26, 2023).

[31] Lorenzo Franceschi-Bicchierai, *Hacker Leaks Millions More 23andMe User Records on Cybercrime Forum*, TechCrunch (Oct. 18, 2023), https://techcrunch.com/2023/10/18/hacker-leaks-millions-more-23andme-user-records-on-cybercrime-forum/ (last accessed Dec. 26, 2023).

The Federal Trade Commission ("FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act.

48. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[32]

49. The FTC recommends that companies verify that third-party service providers have implemented reasonable security measures.[33]

50. The FTC recommends that businesses:

a. Identify all connections to the computers where sensitive information is stored;

b. Assess the vulnerability of each connection to commonly known or reasonably foreseeable attacks;

c. Do not store sensitive consumer data on any computer with an internet connection unless it is essential for conducting their business;

d. Scan computers on their network to identify and profile the operating system and open network services. If services are not needed, they should be disabled to prevent hacks or other potential security problems. For example, if email service or an internet connection is not necessary on a

[32] *Start with Security: A Guide for Business*, Fed. Trade Comm'n (June 2015) https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last accessed Dec. 26, 2023).

[33] Erika Harrell, Bureau Of Just. Stat., U.S. Dep't of Just., NCJ 256085, *Victims of Identity Theft*, 2018 I (2020) https://bjs.ojp.gov/content/pub/pdf/vit18.pdf (last accessed Dec. 26, 2023).

certain computer, a business should consider closing the ports to those services on that computer to prevent unauthorized access to that machine;

e. Pay particular attention to the security of their web applications—the software used to give information to visitors to their websites and to retrieve information from them. Web applications may be particularly vulnerable to a variety of hack attacks;

f. Use a firewall to protect their computers from hacker attacks while it is connected to a network, especially the internet;

g. Determine whether a border firewall should be installed where the business's network connects to the internet. A border firewall separates the network from the internet and may prevent an attacker from gaining access to a computer on the network where sensitive information is stored. Set access controls—settings that determine which devices and traffic get through the firewall—to allow only trusted devices with a legitimate business need to access the network. Since the protection a firewall provides is only as effective as its access controls, they should be reviewed periodically;

h. Monitor incoming traffic for signs that someone is trying to hack in. Keep an eye out for activity from new users, multiple log-in attempts from unknown users or computers, and higher-than-average traffic at unusual times of the day; and

i. Monitor outgoing traffic for signs of a data breach. Watch for unexpectedly large amounts of data being transmitted from their system to an unknown

> user. If large amounts of information are being transmitted from a business's network, the transmission should be investigated to make sure it is authorized.

51. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

52. Upon information and belief, 23andMe failed to properly implement one or more of the basic data security practices described above. 23andMe's failure to employ reasonable and appropriate measures to protect against unauthorized access to consumer PII resulted in the unauthorized release of Plaintiff's and Class Members' PII to the threat actor. Further, 23andMe's failure to implement basic data security practices constitutes an unfair act of practice prohibited by Section 5 of the FTC Act.

53. 23andMe was at all times fully aware of its obligations to protect the PII of consumers because of its business model of collecting PII and storing payment information. 23andMe was also aware of the significant repercussions that would result from its failure to do so.

54. 23andMe's failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data—including extremely sensitive genetic testing information—constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

### *E. Defendant Failed to Comply with the Illinois Genetic Information Privacy Act ("GIPA").*

55. The Illinois Genetic Information Privacy Act ("GIPA") was enacted in 1998 to facilitate the secure, confidential use and disclosure of genetic testing information. 410 ILCS 513/5.

56. GIPA provides that genetic testing and information derived from genetic testing is confidential and privileged, and prohibits the release of said information to anyone that has not been specifically authorized in writing by the individual tested. 410 ILCS 513/15(a).

57. As technology has advanced, GIPA has been amended to keep up with those advancements. In 2018, Illinois legislators amended GIPA to update the definition of "genetic testing" to include "direct-to consumer commercial genetic testing" companies. *See* 410 ILCS 513/10, amended by P.A., 101-0132, § 290, eff. 1/1/2018.

58. As alleged herein, the release of Plaintiff's and Class Members' private information derived from genetic testing is a violation of 410 ILCS 513/15(a) of GIPA.

### *F. Plaintiff and Members of the Class Have Suffered Concrete Injury.*

59. The ramifications of 23andMe's failure to keep PII secure are long-lasting and severe. This is especially the case here, where unlike passwords, credit card numbers, and email addresses that can be compromised in a more typical data breach, the genetic information compromised in the Data Breach cannot be changed.

60. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years. Consumer victims of data breaches are more likely to become victims of identity fraud, occurring 65 percent of the time.[34]

[34] *What Are Your Odds of Getting Your Identity Stolen?*, IdentityForce (Apr. 15, 2021), https://www.identityforce.com/blog/identity-theft-odds-identity-theft-statistics (last accessed Dec. 26, 2023).

61. In 2021 alone, identity theft victims in the United States had financial losses totaling $16.4 billion.[35]

62. Besides the monetary damage sustained, consumers may also spend anywhere from one day to more than six months resolving identity theft issues.[36]

63. Ultimately, the time that victims spend monitoring and resolving identity theft issues takes an emotional toll. Approximately 80% of victims of identity theft experienced some type of emotional distress, and more than one-third of victims experienced moderate or severe emotional distress.[37]

64. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

65. As a result of 23andMe's failure to prevent the Data Breach, Plaintiff and Class Members have suffered and will continue to suffer injuries, including loss of time and productivity through efforts to ameliorate, mitigate, and deal with the future consequences of the Data Breach; theft of their highly valuable PII; the imminent and certainly impending injury flowing from fraud and identity theft posed by their PII being placed in the hands of criminals; damages to and diminution in value of their PII that was entrusted to Defendant with the understanding the Defendant would safeguard the PII against disclosure; and continued risk to Plaintiff's and the Class Members' PII, which remains in the possession of Defendant and which is subject to further

[35] Erika Harrell & Alexandra Thompson, *Victims of Identity Theft, 2021*, U.S. Dept. Just., Bureau Just. Stats. (Oct. 2023), https://bjs.ojp.gov/document/vit21.pdf (last accessed Dec. 26, 2023).
[36] *Id*.
[37] *Id.*

breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the PII with which it was entrusted.

***G. Plaintiff and Members of the Class Are Now at an Increased Risk of Future Harms.***

66. Data Breaches such as the one experienced by Plaintiff and Class Members are especially problematic because of the disruption they cause to the overall daily lives of victims affected by the attack.

67. In 2019, the United States Government Accountability Office ("GAO") released a report addressing the steps consumers can take after a data breach.[38] Its appendix of steps consumers should consider, in extremely simplified terms, continues for five pages. In addition to explaining specific options and how they can help, one column of the chart explains the limitations of the consumers' options. It is clear from the GAO's recommendations that the steps data breach victims (like Plaintiff and Class Members) must take after a Data Breach like 23andMe's are both time-consuming and of only limited and short-term effectiveness.

68. The GAO has long recognized that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[39]

69. The FTC, like the GAO, recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove

[38] Government Accountability Off., "Data Breaches" (Mar. 2019) https://www.gao.gov/assets/gao-19-230.pdf (last accessed Dec. 26, 2023).

[39] *See* "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," Government Accountability Off. (June 2007), https://www.gao.gov/new.items/d07737.pdf ("2007 GAO Report") (last accessed Dec. 26, 2023).

fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[40]

70. Theft of PII is also gravely serious as PII is a valuable property right.[41]

71. It must also be noted there may be a substantial time lag—measured in years—between when harm occurs versus when it is discovered, and also between when SPI is stolen and when it is used. According to the GAO, which has conducted studies 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.[42]

72. PII is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black market" for years.

73. There is a strong probability that the entirety of the stolen information has been or will be dumped on the black market, meaning every Class Member, including Plaintiff, is at an increased risk of fraud and identity theft for many years into the future. Thus, Plaintiff and Class Members must vigilantly monitor their financial and medical accounts for many years to come.

### *H. There Are Multiple Reports of Breached Information Available for Sale on the Dark Web.*

74. Bearing in mind the risks involved with the theft and dissemination of PII, multiple government officials have raised concerns over PII from the Data Breach being posted for sale on the dark web. An inquiry letter issued by Connecticut Attorney General William Tong stated that

---

[40] *See* Identity Theft Victim Checklist, Fed. Trade Comm'n, https://www.identitytheft.gov/Steps (last accessed Dec. 26, 2023).

[41] *See, e.g.*, John T. Soma, et al, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("SPI") Equals the "Value" of Financial Assets*, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("SPI, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

[42] *See* 2007 GAO Report, at 29.

the Data Breach "has resulted in the targeted exfiltration and sale on the black market of at least one million data profiles pertaining to individuals with Ashkenazi Jewish heritage" and mentioned reports indicating "that a subsequent leak has revealed the data of hundreds of thousands of individuals with Chinese ancestry, also for sale on the dark web as a result of this hack."[43]

75. U.S. Senator Bill Cassidy, ranking member of the Senate HELP Committee, also issued an inquiry letter regarding the Breach and his deep concern with its ramifications. In his letter, Senator Cassidy noted that 23andMe "has yet to provide details about when hackers first exploited vulnerability in its systems."[44]

76. With the contextual background of "increasing rates of global antisemitism and anti-Asian hate," Senator Cassidy also cited reports that the threat actor shared the stolen information on a dark web forum where stolen information is frequently posted and sold, listing the information for sale for between $1 and $10.[45]

77. Senator Cassidy's letter refers to a news article that indicates that that the PII "of nearly 7 million 23andMe users was offered for sale on a cybercriminal forum." Specifically, the threat actor claimed that the linked file "contains the profile list of half of the members of 23andMe" along with members' "technical details such as their origin estimation, phenotype and health information, photos and identification data, raw data, and their last login to the site."[46]

---

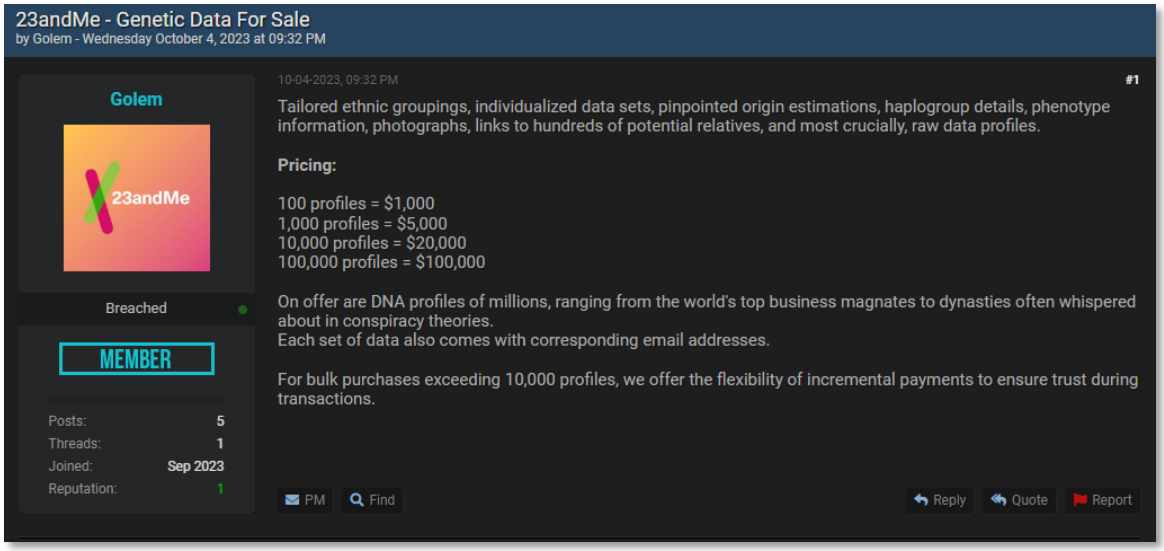
[43] Inquiry Letter from Conn. Att'y Gen. William Tong to 23andMe (Oct. 30, 2023), https://portal.ct.gov/-/media/AG/Press_Releases/2023/10-30-2023-William-Tong--23andMe-Inc-Inquiry-Letter-final-002.pdf (last accessed Dec. 26, 2023).

[44] Inquiry Letter from U.S. Senator Bill Cassidy to 23andMe (Oct. 20, 2023), https://www.help.senate.gov/imo/media/doc/cassidy_letter_on_23andme_data_leak.pdf (last accessed Dec. 26, 2023).

[45] *Id.*

[46] Jonathan Greig, *23andMe Scraping Incident Leaked Data on 1.3 Million Users of Ashkenazi and Chinese Descent*, The Record (Oct. 6, 2023), https://therecord.media/scraping-incident-genetic-testing-site (last accessed Dec. 26, 2023).

78. That is not the only post by the threat actor about 23andMe users' PII. Another post found by investigative reporters listed the pricing for different data sets, advertising "tailored ethnic groupings, individualized data sets, pinpointed origin estimations, haplogroup details, phenotype information, photographs, links to hundreds of potential relatives, and . . . raw data profiles," as well as corresponding email addresses.[47] As seen in the screenshot below, the threat actor listed batches of data for sale to other cybercriminals, with pricing based on the amount of users' data included.[48]




According to the post, the available data ranges from 100 profiles for $1,000 to 100,000 of $100,000.[49]

[47] Bill Toulas, *Genetics Firm 23andMe Says User Data Stolen in Credential Stuffing Attack*, Bleeping Computer (Oct. 6, 2023), https://www.bleepingcomputer.com/news/security/genetics-firm-23andme-says-user-data-stolen-in-credential-stuffing-attack/ (last accessed Dec. 26, 2023).
[48] *Id.*
[49] *Id.*

79. When asked for comment, a spokesperson for 23andMe "confirmed the data is legitimate."[50] However, Defendant's official updated Notice contains no acknowledgment of the availability of PII for purchase nor the associated risks and dangers.

80. That 23andMe users PII is actively being misused and offered for sale on the dark web is indicative of the actual harm Plaintiff and Class's Members have suffered and the certainly impending and increased risk of harm they face as a result of 23andMe's conduct alleged herein.

***I. Plaintiff's Experience.***

81. Plaintiff has been a 23andMe customer since approximately November 3, 2018. Plaintiff purchased a genetic testing kit from 23andMe and thereafter provided Defendant with her sensitive PII. After receiving Plaintiff's genetic testing results from Defendant, Plaintiff opted into 23andMe's DNA Relatives feature. When providing Defendant with her PII, Plaintiff expected that her PII would be kept confidential.

82. On or about October 10, 2023, Plaintiff received a letter from 23andMe informing her that a threat actor had accessed certain individual 23andMe accounts during the Data Breach.

83. On or about October 24, 2023, Plaintiff received a follow-up letter from 23andMe, informing Plaintiff that her PII that she provided to Defendant had been compromised during the Data Breach. Plaintiff did not consent to Defendant's release of her PII to threat actors.

84. Since the Data Breach, Plaintiff has spent numerous hours taking action to mitigate the impact of the Data Breach, which included contacting credit reporting agencies to place a fraud alert and purchasing Allstate identity theft insurance. Plaintiff took these mitigation steps and incurred this loss of time as a direct and proximate result of the Data Breach.

[50] *Id.*

85. Knowing that a threat actor stole her PII, including her genetic information, and knowing that her PII may be available for sale on the dark web, has caused Plaintiff anxiety. She is now very concerned about identity theft and general fraud, and what could happen to her in the future because of the Data Breach. Plaintiff further has concerns and unease about Defendant suffering future data breaches or otherwise releasing Plaintiff's PII in the future.

86. Plaintiff has suffered actual injury from having her PII exposed as a result of the Data Breach, including, but not limited to: (a) paying monies to 23andMe for its genetic testing and ancestry services, goods and services Plaintiff would not have purchased had 23andMe disclosed that it lacked data security practices to safeguard its customers' PII from theft; (b) damages to and diminution in value of her PII—a form of intangible property that Plaintiff entrusted to 23andMe; (c) loss of privacy; (d) lost time; and (e) imminent and impending injury arising from the increased risk of fraud and identity theft.

87. As a result of the Data Breach, Plaintiff will continue to be at a heightened risk for identity theft, and the attendant damages for years to come.

## CLASS ALLEGATIONS

88. Plaintiff brings this action pursuant to Rule 23 of the Federal Rules of Civil Procedure, on behalf of the following class:

> All Illinois citizens whose PII was compromised in the 23andMe Data Breach announced on October 6, 2023 (the "Class").

Excluded from the Class are Defendant, its subsidiaries and affiliates, its officers, directors and members of their immediate families and any entity in which Defendant has a controlling interest, the legal representative, heirs, successors, or assigns of any such excluded party, the judicial officer(s) to whom this action is assigned, and the members of their immediate families. Also excluded from the Class are all persons who seek to arbitrate their claims with Defendant,

notify Defendant of their intention to do so within the Class Period, and do not withdraw that notice within the Class Period. Plaintiff reserves the right to expand, limit, modify, or amend these Class definitions, including the addition of one or more subclass, in connection with their motion for class certification, or at any other time, based upon, *inter alia*, changing circumstances and/or new facts obtained during discovery.

89. **Numerosity.** The class described above is so numerous that joinder of all individual members in one action would be impracticable. The disposition of the individual claims of the respective Class Members through this class action will benefit both the parties and this Court. The exact size of the Class and the identities of the individual members thereof are ascertainable through Defendant's records, including but not limited to, the files implicated in the Data Breach. Defendant has not stated the number of individuals implicated in the Data Breach, but the number is reportedly in the millions.

90. **Commonality.** This action involves questions of law and fact that are common to the Class Members. Such common questions include, but are not limited to:

a. Whether Defendant had a duty to protect the PII of Plaintiff and Class Members;

b. Whether Defendant was negligent in collecting and storing Plaintiff's and Class Members' PII, and breached its duties thereby;

c. Whether Defendant obtained Plaintiff's and Class Members' genetic testing and information derived from genetic testing;

d. Whether Defendant's conduct is subject to GIPA;

e. Whether Defendant released Plaintiff's and Class members' genetic testing and information derived from genetic testing without authorization;

f. Whether Defendant's violations of GIPA were committed intentionally, recklessly, or negligently;

g. Whether Plaintiff and Class Members are entitled to actual damages, statutory damages, and/or other equitable relief as a result of Defendant's wrongful conduct; and

h. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

91. **Typicality.** Plaintiff's claims are typical of the claims of the Class Members. The claims of Plaintiff and Class Members are based on the same legal theories and arise from the same failure by Defendant to safeguard their PII. Plaintiff and Class Members entrusted Defendant with their PII, and it was subsequently released to an unauthorized third party.

92. **Adequacy of Representation.** Plaintiff is an adequate representative of the Class because her interests do not conflict with the interests of the other Class Members Plaintiff seeks to represent; Plaintiff has retained counsel competent and experienced in complex class action litigation; Plaintiff intends to prosecute this action vigorously; and Plaintiff's counsel has adequate financial means to vigorously pursue this action and ensure the interests of the Class will not be harmed. Furthermore, the interests of the Class Members will be fairly and adequately protected and represented by Plaintiff and Plaintiff's counsel.

93. **Superiority.** This class action is appropriate for certification because class proceedings are superior to other available methods for the fair and efficient adjudication of this controversy and joinder of all members of the Class is impracticable. This proposed class action presents fewer management difficulties than individual litigation, and provides the benefits of

single adjudication, economies of scale, and comprehensive supervision by a single court. Class treatment will create economies of time, effort, and expense and promote uniform decision-making.

94. **Predominance.** Common questions of law and fact predominate over any questions affecting only individual Class members. Similar or identical violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that dominate this action. For example, Defendant's liability and the fact of damages is common to Plaintiff and each member of the Class. If Defendant breached its duty and released Plaintiff's and Class Members' PII, then Plaintiff and each Class member suffered damages by that conduct.

95. **Ascertainability:** Members of the Class are ascertainable. Class membership is defined using objective criteria, and Class Members may be readily identified through Defendant's books and records.

## FIRST CAUSE OF ACTION
## NEGLIGENCE
## (On behalf of Plaintiff and the Class)

96. Plaintiff restates and realleges the foregoing allegations as if fully set forth herein.

97. 23andMe owed a duty under common law to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting their PII in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

98. 23andMe had a common law duty to prevent foreseeable harm to others. This duty existed because Plaintiff and Class Members were the foreseeable and probable victims of any inadequate security practices on the part of Defendant. By collecting and storing valuable PII that

is routinely targeted by criminals for unauthorized access, 23andMe was obligated to act with reasonable care to protect against these foreseeable threats.

99. Further, 23andMe had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

100. 23andMe's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because 23andMe is bound by industry standards to protect PII.

101. Upon information and belief, 23andMe alone controlled its technology, infrastructure, and cybersecurity. 23andMe further knew or should have known that if hackers breached its data systems, they would extract sensitive data and inflict injury upon Plaintiff and the Class. Furthermore, 23andMe knew or should have known that if hackers accessed the sensitive data, the responsibility for remediating and mitigating the consequences of the breach would largely fall on individual persons whose data was impacted and stolen.

102. But for 23andMe's wrongful and negligent breach of its duties owed to Plaintiff and Class Members, their PII would not be compromised.

103. As a direct and proximate result of 23andMe's negligence, Plaintiff and Class Members have suffered injury, including:

a. Theft of their PII;

b. Costs associated with the detection and prevention of identity theft and unauthorized use of the financial accounts;

c. Costs associated with purchasing credit monitoring and identity theft protection services;

d. Lowered credit scores resulting from credit inquiries following fraudulent activities;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the 23andMe Data Breach—including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, and engaging in constant vigilance of any fraudulent or criminal activity;

f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PII being placed in the hands of criminals;

g. Damages to and diminution in value of their PII entrusted, directly or indirectly, to 23andMe with the mutual understanding that 23andMe would safeguard Plaintiff's and Class Members' data against theft and not allow access and misuse of their data by others;

h. Continued risk of exposure to hackers and thieves of their PII, which remains in 23andMe's possession and is subject to further breaches so long as 23andMe fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' data;

i. Loss of their privacy and confidentiality in their PII; and

j. Risk of third-party bad actors engaging in certain behavior or taking actions based on Plaintiff's and Class Members' exposed genetic ethnicities.

104. As a direct and proximate result of 23andMe's negligent release of Plaintiff's and Class Members' PII to an unauthorized third party, Plaintiff and Class Members are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

**SECOND CAUSE OF ACTION**
**VIOLATION OF THE ILLINOIS GENETIC INFORMATION PRIVACY ACT, 410 ILCS 513/1, *et seq.***
**(On behalf of Plaintiff and the Class)**

105. Plaintiff restates and realleges the foregoing allegations as if fully set forth herein.

106. GIPA mandates that genetic testing and information derived from genetic testing is confidential and privileged and may be released only to the individual tested and to persons specifically authorized in writing by that individual to receive the information. *See* 410 ILCS 513/15(a).

107. GIPA further provides that [n]o person may disclose . . . the identity of any person upon whom a genetic test is performed or the results of a genetic test in a manner that permits identification of the subject of the test." 410 ILCS 513/30.

108. GIPA provides a private cause of action to any person aggrieved by a violation of the act against any person who negligently, intentionally, or recklessly violates GIPA. 410 ILCS 513/40.

109. 23andMe is a private corporation and thus qualifies as a "person" under GIPA. *See* 410 ILCS 513/10.

110. Plaintiff's PII constitutes genetic testing and information derived from genetic testing under GIPA.

111. By disclosing Plaintiff's and Class Members' PII to the threat actor as alleged above, 23andMe failed to comply with the GIPA mandate to keep information derived from genetic testing confidential and private. 23andMe further failed to receive written authorization before releasing such information to third-party bad actors.[51] *See* 410 ILCS 513/15(a).

112. As a result, GIPA affords Plaintiff and each Class Member a right of action. On behalf of herself and the Class, Plaintiff seeks: (1) injunctive and equitable relief as is necessary to protect the interests of Plaintiff and Class Members by requiring Defendant to comply with GIPA's requirements; (2) statutory damages of $15,000 for each intentional and/or reckless violation of GIPA pursuant to 410 ILCS 513/40(a)(2) or, in the alternative, statutory damages of $2,500 for each negligent violation of GIPA pursuant to 410 ILCS 513/40(a)(1); and (3) reasonable attorneys' fees and costs and other litigation expenses pursuant to 410 ILCS 513/40(a)(3).

## PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and all others similarly situated, prays for relief as follows:

a. For an order certifying the Class under Rule 23 of the Federal Rules of Civil Procedure and naming Plaintiff as representative of the Class and Plaintiff's attorneys as Class Counsel to represent the Class;

b. For an order finding in favor of Plaintiff and the Class on all counts asserted herein;

[51] Courts applying GIPA have consistently noted a difference between its provisions pertaining to disclosure and to release. While Plaintiff is not aware at this time of any facts showing that Defendant affirmatively shared Plaintiff's and Class Members' information, there is no doubt that the information kept on Defendant's service was released to unauthorized individuals. *See, e.g.*, *In re Ambry Genetics Data Breach Litig.*, 567 F. Supp. 3d 1130 (C.D. Cal. 2021); *Tracy v. Elekta, Inc.*, No. 1:21-CV-02851-SDG, 2023 WL 4677021 (N.D. Ga. Mar. 31, 2023).

c. For compensatory, statutory, treble, and/or punitive damages in amounts to be determined by the trier of fact;

d. For an order of restitution, disgorgement, and all other forms of equitable monetary relief;

e. Declaratory and injunctive relief as described herein;

f. Awarding Plaintiff's reasonable attorneys' fees, costs, and expenses;

g. Awarding pre- and post-judgment interest on any amounts awarded; and

h. Awarding such other and further relief as may be just and proper.

**JURY TRIAL DEMANDED**

A jury trial is demanded on all claims so triable.

Dated: December 26, 2023

Respectfully submitted,

*/s/ Katrina Carroll*
Katrina Carroll
**LYNCH CARPENTER, LLP**
111 W. Washington St.
Suite 1240
Chicago IL 60602
312.750.1265
katrina@lcllp.com

Jonathan M. Jagher
**FREED KANNER LONDON & MILLEN LLC**
923 Fayette Street
Conshohocken, PA 19428
610.234.6486
jjagher@fklmlaw.com

Michael E. Moskovitz
Nia-Imara Barberousse Binns
**FREED KANNER LONDON & MILLEN LLC**
100 Tri-State International, Suite 128
Lincolnshire, IL 60069
224.632.4506
mmoskovitz@fklmlaw.com

nbinns@fklmlaw.com

**Attorneys for Plaintiff and the Proposed Class*