IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

BRENDA LIANG, O.D., JESSICA OLENDORFF, O.D., KRISTINE FERGASON, O.D., JULIE WOLF, O.D., CAMILLA DUNN, O.D., MARK GARIN, O.D., NATALIE WEST, ANDREA ROBINSON, O.D., PRISCILLA PAPPAS-WALKER, O.D., and LAUREN NELSON, O.D., on behalf of themselves and all others similarly situated,

Plaintiffs,

v.

NATIONAL BOARD OF EXAMINERS IN OPTOMETRY, INC.,
351 West Camden Street
Baltimore, Maryland 21201
Baltimore County

Defendant.

CASE NO. 1:17-CV-1964

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Plaintiffs Brenda Liang, O.D., Jessica Olendorff, O.D., Kristine Fergason, O.D., Julie Wolf, O.D., Camilla Dunn, O.D., Mark Garin, O.D., Natalie West, Andrea Robinson, O.D., Priscilla Pappas-Walker, O.D., and Lauren Nelson, O.D. (collectively "Plaintiffs"), individually and on behalf of the classes of similarly situated persons defined below, allege the following against the National Board of Examiners, its agents, and all persons or entities acting on its behalf or at its direction or control ("NBEO" or "Defendant"). Plaintiffs make these allegations upon personal knowledge with respect to themselves and on information and belief derived from, among other things, investigation of counsel and review of public documents as to all other matters.

NATURE OF THE ACTION

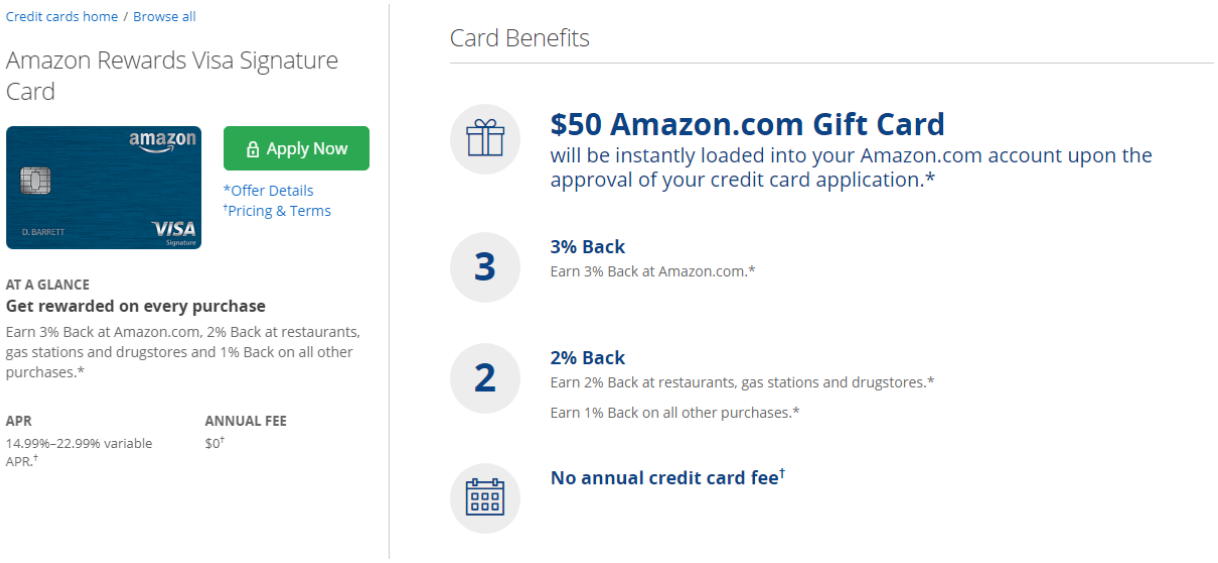
1. The NBEO is the testing organization in the field of optometry in the United States of America (including Puerto Rico). The organization creates and administers various exams in the optometry profession. As part of its exam administration process, the NBEO collects the personal identifying and financial information of exam-takers, including but not limited to names, birth dates, Social Security numbers, addresses, and credit card information ("Personal Information").

2. The NBEO, or a party within its control, suffered a data breach involving the Personal Information of exam-takers and other individuals, the full extent of which is still unknown. The fraud resulting from this data breach is as extensive as any data breach in history, with an alarming percentage of optometrists practicing in the United States having already suffered identity theft and fraud. The damage resulting from this breach is extensive and ongoing. NBEO is the only known common source of the breached data,

and it had a non-delegable duty to maintain reasonable and adequate security measures to safeguard Plaintiffs' Personal Information.

3. On or around July 23, 2016, optometrists from around the country began to notice that fraudulent accounts were being applied for and/or opened in their names with JPMorgan Chase Bank, N.A. ("Chase"). They started discussing it on Facebook groups formed for the purpose of identifying the source of the breach and soon realized they were all victims of the same type of fraud. In particular, many optometrists learned that a Chase Amazon Visa credit card had been applied for in their name using their Social Security numbers, and all within a few days of one another. The optometrists soon realized that the only common source amongst them and to which they had all given their Personal Information that included Social Security numbers and dates of birth (information necessary to apply for new lines of credit, among other things), was the NBEO, where every graduating optometry student has to submit their Personal Information to sit for board-certifying exams.

4. Fraudsters engaged in this scheme because it was a fast and simple way to take advantage of a promotion offered by Amazon, whereby enrollees received a free $50 in their Amazon account upon applying for a Chase Amazon Visa credit card. The fraudsters would use victims' real information to apply for a Chase Amazon credit card, and then link the card to a dummy Amazon account where the fraudster would receive a free $50. The victims would then receive a copy of the unauthorized credit card at their home address or whatever address was linked to the victim's NBEO account.



5. The breach also affected optometrists who served as examiners or committee members for NBEO and optometrists who later sat for additional NBEO competency exams well after graduating from optometry school. Individuals that submitted their Personal Information to NBEO even more than 30 years ago have been affected. Many victims provided NBEO with unique information compromised in the breach that was not provided to other professional organizations.

6. Subsequently, the fraud has expanded from Chase accounts to multiple other forms of fraud. In particular, while optometrists are continuing to this day to learn that Chase Amazon Visa cards are being applied for in their names, many are also learning that other accounts are being fraudulently applied for and/or opened in their names, including GreenDot debit cards, PayPal business accounts, Synchrony Bank cards, and Discover cards using personal information contained in NBEO's data systems (and for many, in *only* NBEO's data systems). Some have also had fraudulent tax returns

filed in their names, fraudulent charges made on existing credit cards, and their identities stolen to obtain medical care.

7. Despite receiving multiple contacts from affected individuals informing NBEO that the information used to open fraudulent accounts was information contained *only* in NBEO's systems, NBEO has failed to provide notice of the breach to the breach victims and has affirmatively denied its responsibility for the breach.

8. Plaintiffs are individuals who submitted their Personal Information to the NBEO as part of the exam-administration process and whose Personal Information has been compromised as a result of the NBEO's failure to maintain reasonable and adequate security measures to safeguard their Personal Information. Plaintiffs are seeking damages, restitution, and injunctive relief requiring NBEO to notify affected individuals of the breach of its data and to implement and maintain reasonable and effective security practices.

PARTIES

9. Plaintiff Brenda Liang, O.D., is an optometrist residing in Valley Stream, New York. She submitted Personal Information to NBEO as part of NBEO-administered exams taken in 2013, 2014, and 2015. Plaintiff Liang's Personal Information was compromised during the NBEO data breach. Specifically, on August 28, 2016, August 29, 2016, and November 8, 2016, fraudsters applied for Chase Amazon Visa credit cards using Plaintiff Liang's stolen Personal Information. All three card applications were cancelled before they were approved because Plaintiff Liang had already placed credit freezes with the three major credit reporting agencies. On September 17, 2016, a

fraudulent charge was made on Plaintiff Liang's Bank of America credit card in the amount of $1,247.23 to Woot Inc., an on-line retailer. On September 19, 2016, three fraudulent Macys.com orders for men's shoes were made using Plaintiff Liang's Personal Information in the amounts of $234.97, $379.98, and an unknown amount resulting in her Macys.com account being overdrawn. Plaintiff Liang also subsequently received a fraudulent NASCAR reloadable prepaid Visa card that was opened using her Personal Information, and learned that a PayPal account was fraudulently opened using her Personal Information. A fraudulent eBay order was also made on Plaintiff Liang's account. Plaintiff Liang was harmed by having her Personal Information compromised and having fraudulent charges made using her Personal Information. Plaintiff Liang subsequently learned that additional attempts have been made to open fraudulent Chase Amazon applications in her name. Plaintiff Liang has spent time and money putting credit freezes and fraud alerts in place with the credit reporting agencies Experian, TransUnion, and Equifax, filing a police report, notifying the IRS of the compromise of her Social Security number, and purchasing a LifeLock UltimatePlus account for identity theft protection for over $300 per year. Plaintiff Liang also faces the imminent and certainly impending threat of future additional harm from the increased threat of identity theft and fraud due to her Personal Information being sold on the Internet black market and/or misused by criminals.

10. Plaintiff Jessica Olendorff, O.D., is an optometrist residing in Saint Charles, Missouri. She submitted Personal Information to NBEO as part of NBEO-administered exams taken in 2013 and 2014. Plaintiff Olendorff's Personal Information

was compromised during the NBEO data breach. In particular, on August 3, 2016, a fraudster applied for a Chase Amazon Visa credit card using her Personal Information. She called Chase and reported the application as fraudulent, put an alert on her account, and requested that the inquiry be removed from her credit report. At the same time, she also froze her credit with all three credit reporting agencies. On December 14, 2016, a fraudulent charge of $178.79 was made to Plaintiff Olendorff's U.S. Bank Visa Card from "PFA *GUHONG Co., LTD." In February 2017, a fraudulent charge of approximately $500 was made to her US Bank Cash+ Visa Signature Card from Nordstrom. On March 11, 2017, a fraudulent charge of $91.50 was made to her U.S. Bank Visa Check Card from Country Club Hill Cinema, and the same day a fraudulent charge of $88.50 was made on the same card from Chicago Heights Cinema. That same day, multiple, rapid attempts were made for additional movie tickets, but her bank identified the transactions as suspicious and blocked them. On March 23, 2017, a fraudster applied for another Chase Amazon Visa credit card using Plaintiff Olendorff's Personal Information. The application was denied because Plaintiff Olendorff had previously frozen her credit. The information used to apply for both fraudulent Chase Amazon Visa cards was Plaintiff Olendorff's parent's address and phone number that she used in optometry school. They also used her married name. Plaintiff Olendorff was married in 2013. Plaintiff Olendorff updated other optometric associations with her current information after graduation, but never had any need to update NBEO. Thus, the only optometric association that still had that combination of information was NBEO. Plaintiff Olendorff also faces the imminent and certainly impending threat of future

additional harm from the increased threat of identity theft and fraud due to her Personal Information being sold on the Internet black market and/or misused by criminals.

11. Plaintiff Kristine Fergason, O.D., is an optometrist residing in Los Altos, California. She submitted Personal Information as part of exams taken through the NBEO in approximately 1994, 1995, and 1996. Plaintiff Fergason also served as a clinical examiner for NBEO from approximately 1998-2008. Plaintiff Fergason's Personal Information was compromised during the NBEO data breach. In particular, Plaintiff Fergason had multiple Chase Amazon Visa credit card applications opened in her name, with the most recent being March 2017. Plaintiff Fergason was harmed by having her Personal Information compromised and now faces the imminent and certainly impending threat of future additional harm from the increased threat of identity theft and fraud due to her Personal Information being sold on the Internet black market and/or misused by criminals. Plaintiff Fergason also has spent time and money putting credit freezes and fraud alerts in place with the credit reporting agencies Experian, TransUnion, and Equifax, notifying the federal government of the compromise of her Social Security number, and purchasing a LifeLock account for identity theft protection for nearly $297 per year.

12. Plaintiff Julie Wolf, O.D., is an optometrist residing in Inlet Beach, Florida. She submitted Personal Information as part of exams taken through the NBEO in 1992, 1993, and 1995. Plaintiff Wolf's Personal Information was compromised during the NBEO data breach. In particular, on July 23, 2016, a Chase Amazon Visa credit card was applied for using Plaintiff Wolf's maiden name (Galbreath), and a prior Alpharetta,

Georgia address. A hard pull credit inquiry appeared on Plaintiff Wolf's credit reports with both Experian and Equifax. Chase denied the application because she had two existing Chase accounts in her married name. A few years ago, Plaintiff Wolf contacted the NBEO because she was applying for a new state license and had to forward her scores to that state's certification board. At that time, she updated her address in NBEO's systems to the Alpharetta address used in the fraudulent application. She moved from the Alpharetta address on October 31, 2015. Additionally, she had not used her maiden name since 1999 but never updated that information in NBEO's system. NBEO is the only optometric association that had the combination of Plaintiff Wolf's maiden name and her Alpharetta address in its systems. Plaintiff Wolf faces the imminent and certainly impending threat of future additional harm from the increased threat of identity theft and fraud due to her Personal Information being sold on the Internet black market and/or misused by criminals. Plaintiff Wolf also has spent time and money placing fraud alerts and credit freezes with the three major credit reporting agencies, notifying the Federal Trade Commission (FTC) and Internal Revenue Service (IRS) of the fraud, calling and writing Chase requesting that it notifies the credit reporting agencies that the credit inquiry was based on a fraudulent application, submitting inquiry disputes with Experian and Equifax (to no avail, the credit inquiry is still on both credit reports), opting out of receiving credit card offers, calling her banks and credit card companies to put fraud alerts on her accounts along with a multi-step verification process, alerting the Social Security fraud department and Chexsystems, and contacting PayPal to ensure no fraudulent accounts have been opened using her Personal Information.

13. Plaintiff Camilla Dunn, O.D., is an optometrist residing in Palm Bay, Florida. She submitted her Personal Information to NBEO as part of exams taken through NBEO in 1997, 1998 and 2000. Plaintiff Dunn's Personal Information was compromised during the NBEO data breach. Plaintiff Dunn heard from her classmates about the fraud many of them were experiencing and began calling Chase every week to determine whether she was affected. In September 2016, Plaintiff Dunn learned that fraudsters had applied for a Chase credit card using Plaintiff Dunn's Personal Information. She immediately reported it as fraud to have the application cancelled. The information used to apply for the card included Plaintiff Dunn's maiden name (Quirie) and an address that Plaintiff Dunn lived at for only one year during her optometry residency in Columbus, Ohio. Only NBEO had the combination of Plaintiff Dunn's maiden name and her Columbus, Ohio address in its systems. Plaintiff Dunn has spent time and money putting fraud alerts and credit freezes in place and filing a police report with her local law enforcement. She also faces the imminent and certainly impending threat of future additional harm from the increased threat of identity theft and fraud due to her Personal Information being sold on the Internet black market and/or misused by criminals.

14. Plaintiff Mark Garin, O.D., is an optometrist residing in Birmingham, Michigan. He submitted Personal Information as part of exams taken through the NBEO in 1983, 1984, and 1985. Plaintiff Garin's Personal Information was compromised during the NBEO data breach. An email blast was sent to all optometrists in Michigan in late July 2016 from the Michigan Optometric Association alerting them of the rampant fraud being perpetrated on the optometry profession and requesting that optometrists be

vigilant for identity theft. It advised optometrists to set up credit alerts and also to freeze their credit with Experian, Equifax and TransUnion. Plaintiff Garin set up credit monitoring and added credit freezes on August 14, 2016 as more and more optometrists reported that they had been the victims of fraud. The Michigan Optometric Association gave the optometrists a toll-free number associated with the Chase Amazon card: 888-247-4080. The instructions were to press #, then 3, then 1 to see if a card was in process under the optometrist's Social Security number. Plaintiff Garin did this each day since the warning email came in July 2016. He had no activity until October 6, 2016, when he was informed by recording that an application had been made for a Chase Amazon Visa credit card using his Social Security number. He was then transferred to a Chase agent who confirmed that someone used his Social Security number and date of birth to apply for the card. An agent in Chase's fraud department subsequently confirmed that the address used to apply for the card matched the one Plaintiff Garin lived at when he took NBEO's board exam in 1986: 2052 Winchester Road, Rochester, Michigan 48307. He lived at that address for only 18 months between 1986 and 1988. The fraudsters used the now defunct zip code for that address (48063) rather than the new one established for that locality in approximately 1988 (48307). Additionally, in April 2017, Plaintiff Garin learned that another fraudulent Chase Amazon Visa credit card application had been submitted using his Personal Information, which he was able to detect by diligently monitoring his accounts. Plaintiff Garin continues to extensively monitor his accounts for ongoing fraud. Plaintiff Garin faces the imminent and certainly impending threat of future additional harm from the increased threat of identity theft and fraud due to his Personal Information

being sold on the Internet black market and/or misused by criminals. Plaintiff Garin also has spent time and money putting fraud alerts and credit freezes in place. These protective measures recently made it very difficult for Plaintiff Garin to lease a car and to get a new credit card.

15. Plaintiff Natalie West is an optometry student residing in Birmingham, Alabama, attending the University of Alabama at Birmingham School of Optometry. She submitted Personal Information to NBEO in the spring of 2016 but has yet to sit for board exams. Plaintiff West's Personal Information was compromised during the NBEO data breach. Plaintiff West was approved for and received a Chase Amazon Visa credit card at the end of July 2016 that she did not apply for. She contacted the Chase fraud department to report the card as fraud and to have the account deleted. She also submitted a report online to the FTC and placed a fraud alert on her credit through the three national credit reporting agencies. The only optometric association that Plaintiff West gave her Social Security number to was the NBEO. The fraudsters used Plaintiff West's full Social Security number when applying for the fraudulent Chase Amazon Visa card. Plaintiff West faces the imminent and certainly impending threat of future additional harm from the increased threat of identity theft and fraud due to her Personal Information being sold on the Internet black market and/or misused by criminals.

16. Plaintiff Andrea Robinson, O.D. is an optometrist residing in Chesterfield, New Jersey. She submitted Personal Information as part of exams taken through the NBEO in 2004-2006. Plaintiff Robinson's Personal Information was compromised during the NBEO data breach. Plaintiff Robinson received a call from Chase on April 4, 2017

informing her that a Chase Amazon Visa credit card had been applied for in her name. She informed Chase that the account was fraudulent and notified the three national credit reporting agencies of the fraud. Plaintiff Robinson is not a member of any other optometric association; no optometric association besides the NBEO has Plaintiff Robinson's Social Security number, which was necessary to apply for the Chase Amazon Visa card. Plaintiff Robinson also faces the imminent and certainly impending threat of future additional harm from the increased threat of identity theft and fraud due to her Personal Information being sold on the Internet black market and/or misused by criminals.

17. Plaintiff Priscilla Pappas-Walker, O.D., is an optometrist residing in Maroa, Illinois. She submitted Personal Information as part of exams taken through the NBEO in approximately 2007, 2008, and 2009. Plaintiff Pappas-Walker's Personal Information was compromised during the NBEO data breach. In particular, Plaintiff Pappas-Walker learned of colleagues who had had fraudulent Chase Amazon Visa accounts applied for and opened in their names. Accordingly, she had been periodically checking with Chase to see if any applications had been initiated, but every time she called, she was informed that no such applications were pending. On September 22, 2016, however, Chase sent a letter to Plaintiff Pappas-Walker's parents' address stating that an application had been received for an Amazon Chase Visa credit card in Plaintiff Pappas-Walker's name. The letter was sent using Plaintiff Pappas-Walker's maiden name, Priscilla Pappas. Chase denied the application. Plaintiff Pappas-Walker had previously changed the repayment terms on one of her largest student loans to pay it off quicker and thus had used a lot of

her available credit at the time. She immediately contacted Chase to report the fraud. Chase said it would notify the credit reporting agencies, but she called all three herself to confirm the fraud alerts were actually in place. Plaintiff Pappas-Walker deferred refinancing some of her other student loans, as well as her husband's because of the hassle of having the fraud alert on her credit. She enrolled in LifeLock for both herself and her husband to safeguard against further fraudulent activity. The "hard inquiry" that resulted from the fraudulent credit application was still appearing on Plaintiff Pappas-Walker's Experian credit report months after the fact, causing Plaintiff Pappas-Walker to spend significant time and effort attempting to have it removed or otherwise risk further damaging her credit. Plaintiff Pappas-Walker was alerted by LifeLock that another fraudulent Chase Amazon Visa credit card application had been submitted on April 7, 2017. She again reported the application as fraud to Chase and the credit reporting agencies and initiated 90-day fraud alerts with the credit reporting agencies. The fraudsters used Plaintiff Pappas-Walker's maiden name and parents' address — the same information she used to register for exams with NBEO. She provided the Illinois Optometric Association and the American Optometric Association (AOA) with her new name after she was married in 2014, and she had updated her address with those organizations in 2013. She never updated any of her information with NBEO because the board exams were long over and it seemed unnecessary as NBEO is not an active organization like AOA. After experiencing the identity theft described above, Plaintiff Pappas-Walker confirmed that NBEO still maintains in its systems her prior name and address that were used to commit fraud. On June 21, 2017, Plaintiff Pappas-Walker was

notified by LifeLock that a second Amazon Chase Visa credit card had been applied for in her name. Plaintiff Pappas-Walker had a "hard inquiry" on her credit report relating to the fraudulent application and had to contact Chase and the credit reporting agencies to report the fraud, including adding a new fraud alert to her credit report. Plaintiff Pappas-Walker also faces the imminent and certainly impending threat of future additional harm from the increased threat of identity theft and fraud due to her Personal Information being sold on the Internet black market and/or misused by criminals.

18. Plaintiff Lauren Nelson, O.D., is an optometrist residing in Houston, Texas. She submitted Personal Information as part of exams taken through the NBEO in March 2010, December 2010, and April 2011. Plaintiff Nelson's Personal Information was compromised during the NBEO data breach. On August 2, 2016, Plaintiff Nelson called Chase to check for fraudulent activity after being warned by a former classmate that optometrists were targets of a widespread fraud scheme. Plaintiff Nelson learned that a Chase Amazon Visa credit card had already been opened in her name and mailed to her parents' former address, the same address she submitted to NBEO to sit for the exams. Plaintiff Nelson contacted the credit reporting agencies to put a credit freeze on her accounts, filed a police report in Houston, Texas, and changed the passwords on all of her email and financial accounts. Plaintiff Nelson also filed a complaint with the FBI's Internet Crime Complaint Center (IC3) and notified the IRS. On August 3, 2016, Plaintiff Nelson formed the Facebook Group called "Eyedentitytheft2016" in order to create an online forum where optometrists could gather to share information and advice about their experiences relating to the NBEO data breach. To date, the group has more than 4,530

members. On August 4, 2016, Plaintiff Nelson logged into her accounts with NBEO, the Association of Regulatory Boards of Optometry (ARBO), and additional optometry groups and confirmed that only the information she submitted to NBEO was consistent with the out-of-date information used on the fraudulent credit application. Plaintiff Nelson has spent significant time and money investigating the fraud, filing police reports, contacting the IRS and FBI, mailing documentation necessary to implement credit freezes, and hosting a Facebook group that thousands of individuals have joined to discuss fraud linked to the NBEO. Plaintiff Nelson, like thousands of others, also faces the imminent and certainly impending threat of future additional harm from the increased threat of identity theft and fraud due to her Personal Information being sold on the Internet black market and/or misused by criminals.

19. Defendant the National Board of Examiners in Optometry, Inc. is a privately-held not-for-profit corporation. The NBEO is incorporated in Maryland with its principal office located at 351 West Camden Street, Baltimore, Maryland 21201, and maintains its principal place of business in North Carolina at 200 S. College Street, Suite 2010, Charlotte, North Carolina 28202.

JURISDICTION AND VENUE

20. This Court has jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million exclusive of interest and costs. At least one Plaintiff and Defendant are citizens of different states. There are more than 100 putative class members.

21. This Court has jurisdiction over the NBEO because it is incorporated in Maryland and avails itself to Maryland.

22. Venue is proper in this District under 28 U.S.C. § 1391 because the NBEO is a resident of this District.

FACTUAL ALLEGATIONS

The NBEO Collects Significant Amounts of Consumer Information

23. Established in 1951, the NBEO is the testing organization in the field of optometry in the United States of America (including Puerto Rico). The organization creates and administers various credentialing exams in the optometry profession, and passing its exams is necessary for an optometrist to be licensed to practice. NBEO states that its "mission is to protect the public by accurately assessing the competence of practicing optometrists."[1]

24. Prospective optometrists pay the NBEO to take at least three credentialing exams required for the optometry profession. The Part I examination, entitled "Applied Basic Science" (ABS), tests the underlying basic science concepts necessary to enter the clinical practice of optometry. The Part II exam tests on "Patient Assessment and Management" (PAM), and the Part III exam tests clinical skills. The NBEO also offers advanced examinations. Below is the fee schedule for the various exam administration services offered by NBEO:

[1] http://www.optometry.org/president.cfm.

Examination fees are payable at the time of online registration, and candidates may usa a credit or debit/check card , or eCheck.

$725	Part I (Applied Basic Science)
$725	Part II (Patient Assessment and Management)
$725	Part III (Clinical Skills)
$450	TMOD
$500	CPDO
$780	ACMO (*There is a special reduced fee of **$480** for current residents who sit for the exam during the year in which they complete their residency.*)
$250	Injections Skill Examination (ISE)
$25 $100	Online State Law Exam (OSLE)* In-house State Law Exam*
$400	Late Registration Fee*

*** Fees are non-refundable**

SCORE VERIFICATION FEES		
Part I (ABS)	**$60**	(sessions 1 & 2)
Part II (PAM)	**$60**	(sessions 1 & 2)
TMOD (stand-alone)	**$30**	(session 1)
ACMO	**$30**	(session 1)

25. In a notice available on its website, the NBEO states that it gathers, uses and shares the personal information of exam-takers.[2] The notice provides that the NBEO "gather[s] your personal information from our Web site Application and use[s] this information to respond and fulfill your requests with the NBEO."[3] The NBEO "may share segments of your personal information with our affiliated organizations to complete a transaction you specifically request. The information we share are name, address, last 4-

[2] https://www.optometry.org/privacy.cfm (last visited July 5, 2017).

[3] *Id.*

digits of social security number, oe tracker number, birth year, scores, and graduation year."[4]

26. The NBEO acknowledges that exam-takers' Personal Information is highly sensitive and that it has a duty to safeguard and secure such information. The NBEO states on its website:

> **How your Personal Information is Protected**
>
> NBEO has implemented a variety of encryption and security technologies and procedures to protect information stored in our computer systems from unauthorized access. We reveal only the last 4 digits of your credit card number when confirming orders as well as maintaining procedural safeguards that restrict your personal information to employees (or individuals working on our behalf and under confidentiality agreements) who need to know your personal information in order to provide products and/or services that you request.
>
> We use 128-bit encryption technology and Secure Socket Layers ("SSL") in all areas where your personal and account information is required. Our Web site is certified by VeriSign, which verifies that our Web site is authentic and that we use SSL security.[5]

27. In addition to its substantial current exam-taker database, the NBEO also stores and maintains the Personal Information of previous exam-takers–even years after their relationship with the NBEO has ended.

[4] *Id.*

[5] http://www.optometry.org/privacy.cfm. Sometime after being notified of the breach, NBEO updated the policy to state "We use 256-bit encryption technology . . . in all areas where your personal and account information is required."

The NBEO Data Breach

28. On or about July 23, 2016, optometrists from around the country began noticing fraudulent Chase Amazon Visa credit card accounts were being opened in their names. Numerous optometric associations reported on the issue.[6]

29. Optometrists started discussing the problem online and in various Facebook groups and they soon discovered that NBEO was the only common link amongst them. In particular, each optometrist who had learned of a fraudulent credit application in their name had submitted their Personal Information, including Social Security number, to NBEO. Other potential common links shared by optometrists could be affirmatively excluded as the source of the breach. The American Optometric Association (AOA) does not gather or store Social Security numbers. The American Academy of Optometry (AAO) does not store Social Security numbers, and many optometrists affected by the fraud do not have records in AAO's database. Similarly, the Association of Regulatory Boards of Optometry (ARBO) confirmed that some of the individuals affected are not in its database. In addition, numerous optometrists had cards applied for and/or opened

[6] *See, e.g.*, Credit breach continues grip on optometrists, students, available at http://www.aoa.org/news/practice-management/credit-breach-continues-grip-on-optometrists-students?sso=y (Sept. 1, 2016); Optometrists and Optometric Students Are Targets of Far-Reaching Data Breach, available at http://www.visionmonday.com/latest-news/article/optometrists-and-optometric-students-are-targets-of-farreaching-data-breach-1-1 (Aug. 5, 2016); Developing story: ODs targeted for credit fraud, available at http://optometrytimes.modernmedicine.com/optometrytimes/news/developing-story-ods-targeted-credit-fraud (Aug. 2, 2016); American Optometric Association Warns Optometrists of Credit Fraud Risk, available at http://www.hipaajournal.com/american-optometric-association-warns-optometrists-of-credit-fraud-risk-3549/ (Aug. 11, 2016); Nationwide Data Breach Affecting Optometrists, available at http://www.aaopt.org/notice-nationwide-data-breach-affecting-optometrists (Aug. 11, 2016).

using information that only existed in NBEO's systems. Literally thousands of optometrists have congregated online to discuss the fraud they have already experienced, with the only common source of the compromised data being NBEO.

30. When alerted to the issue by the affected optometrists, the NBEO denied its responsibility for the fraud for several days, but on August 4, 2016, the NBEO issued a statement on its website stating that it had "decided further to investigate whether personal data was stolen from [its] information systems to support the perpetrators' fraud on individuals and Chase."

31. Also on August 4, 2016, Plaintiff Nelson wrote an email to NBEO:

> To whom it may concern:
>
> As I know you are well aware, the personal information of optometrists across the country has been compromised from what appears to be a breach of an optometry database. I believe you are being aggressive in your statement of innocence without an outside security expert being used. Please correct me if I am wrong in assuming that you have only performed an internal investigation by those who normally handle your information security.
>
> I am in no way assigning guilt or assuming guilt, but I feel that as the holder of the confidential information being utilized to open new Chase Amazon.com credit cards, you owe all parties involved your due diligence in performing an investigation of your security measures that includes an examination by an outside source that has not previously been involved in setting up or maintaining your database. A good hacker can leave no evidence that is recognizable by someone not well-trained in looking for a breach.
>
> What is your response to the fact that many people, like myself, had the credit card applied for with an outdated address that is seemingly only still on file with you? My current address is listed with AOA, TOA, my license, and the insurance panels I am on/CAQH. The address on file with ARBO is an older one that is different from the one you have on file which was used for the card. Those that have had updated information used to apply for the

> Chase card seem to have in some way been affiliated with you recently and updated addresses with you due to getting re-licensed in new states and requiring scores.
>
> Why is it necessary for you to store our social security numbers in the first place? Why was a different unique identifier not utilized by you to keep track of us?
>
> What type of encryption is used in your database and who maintains it?
>
> What type of examination of your systems did you perform in order to ensure that the breach was not yours before making a statement declaring that there is "no evidence whatsoever" indicating that your system was involved?
>
> These are all questions that I feel those of us affected are owed answers to. I appreciate you taking the time to read my questions and respond at your earliest convenience. I am also strongly urging you to have an outside, independent audit performed if you have not already done so.
>
> Thank you,
>
> Lauren Nelson, OD

32. Plaintiff Nelson followed up with a second email to NBEO on August 5, 2016 noting that based on at least two examples, the breach likely occurred sometime between October 2015 and mid-June 2016.

33. On August 25, 2016, NBEO updated its statement with a message stating its internal review was still ongoing and that it may take a "number of additional weeks to complete," and continued to advise affected individuals to "remain vigilant" in checking their credit.

34. On August 31, 2016, Dr. Jack Terry, the Chief Executive Officer of NBEO, responded to Plaintiff Nelson by email, but failed to address many of the issues raised in Plaintiff Nelson's prior correspondence:

Dear Dr. Nelson,

Thank you for contacting me about your concern that individuals in the optometry community have been the victims of identity thefts in which fraudulent applications for Chase credit cards have been submitted under their names. I trust you received my August 18 email responding to your concern, and I'm writing again to give you an update on the situation.

I share your frustration over the inconvenience and anxiety this crime has caused our community, as well as over the time it is taking to determine the source of the stolen information.

As we reported on August 4, the NBEO has retained a law firm, which with the assistance of a nationally-known cybersecurity firm, is investigating whether the security of NBEO databases has been breached. We initiated this intensive response within 48 hours of receiving reports from a number of optometrists and optometry students that Chase credit cards, particularly Visa cards co-marketed with Amazon, had been fraudulently applied for under their names.

The internal review that NBEO has commissioned is necessarily painstaking. Cyber-attackers today rely on sophisticated means that can render intrusions indistinguishable from ordinary and secure network operations. While cybersecurity experts are, on occasion, able to confirm an intrusion in mere days, often more evidence and analysis is necessary before a determination may become feasible. That is the case here.

The investigators have already collected and analyzed large volumes of NBEO's data. Analysis to date, however, does not establish whether an intrusion in fact occurred. Collection and technical analysis is therefore continuing, involving still more data, both current and retrospective.

We are not the only organization that maintains records containing the personal identifiers of individual victims of the fraudulent scheme. Moreover, we are a not-for profit organization that supports the missions of state licensing boards by developing and administering standardized examinations, funded solely by testing fees. It is therefore especially important that NBEO not assume or speculate that its data security was breached. Rather, in seeking to determine if a breach within NBEO occurred, we must be guided by hard evidence. Our best source of such evidence is the continuing internal inquiry.

> Depending on what that inquiry reveals and when, it could take a number of additional weeks to complete. If at any juncture, however, the inquiry establishes that NBEO's systems were breached, we will promptly notify affected parties as the law requires and undertake other security measures as appropriate.
>
> We share with the entire optometric community frustration at the uncertainty and alarm that the perpetrators have spread through their crimes. We urge you and your optometric colleagues to remain vigilant, taking the steps that we and other organizations have previously emphasized: establishing fraud alerts or freezes; periodically inquiring of Amazon Chase whether fraudulent applications have been made in your name; and regularly checking your credit history.
>
> We will continue to provide updates on our website as this matter develops.
> Sincerely,
>
> Dr. Jack Terry
>
> Chief Executive Officer

35. On September 26, 2016, a survey was posted in an optometry Facebook group seeking information regarding the scope of the harm caused by the data breach. In less than 12 hours, 983 optometrists or optometry students submitted responses. Out of that group, 830 stated that they were recently affected by identity theft, and the overwhelming majority of respondents indicated that the address used to perpetrate the fraud was the address used to register for board exams with the NBEO or an address otherwise provided to NBEO before the identity theft occurred.

36. On January 26, 2017, after months of silence, NBEO stated that its forensic investigation "found no evidence of a compromise of personal information within NBEO's care."[7] NBEO provided no further details about its purported investigation, nor

[7] http://www.optometry.org/.

does NBEO's statement indicate whether it allowed agents or contractors to access its systems and whether any investigation had been conduct as to whether such agents' systems had been breached.

37. Plaintiffs have repeatedly requested that NBEO produce the results of its "forensic investigation" – to which NBEO has steadfastly refused. NBEO has never notified affected individuals that their Personal Information was compromised, even though there is overwhelming evidence that NBEO or a party acting under its control was breached.

38. As a result of NBEO's delay in notifying potentially affected individuals, many class members will be unaware that their Personal Information has been compromised and will not timely take the steps necessary to safeguard themselves from the improper use of that information.

NBEO Failed to Maintain Reasonable and Adequate Security Measures to Safeguard Consumers' Information

39. NBEO's failure to provide adequate security measures to safeguard exam-takers' information is especially egregious because NBEO operates in the education field which has recently been a frequent target of scammers attempting to fraudulently gain access to students' and employees' confidential personal information.

40. In fact, NBEO has been on notice for years that the education system is a prime target for scammers because of the amount of confidential employee and student records maintained. In 2014 and 2015 alone, numerous higher education institutions suffered high-profile data breaches including the University of Maryland, North Dakota

University, Butler University, Indiana University, Arkansas State University, Pennsylvania State University, Washington State University, Harvard University, Johns Hopkins University, the University of Virginia, and the University of Connecticut, among many others.

41. According to a Privacy Rights Clearinghouse study entitled "Just in Time Research: data breaches in Higher Education," the higher education industry accounted for 17% of all reported data breaches in the last decade, second only to the medical industry with 27%.

42. From 2005-2014, there were more than 727 publicized breaches involving educational institutions, compromising at least 14 million personal records.

43. NBEO was aware, or should have been aware, that it was a target for fraudsters yet failed to implement basic cyber-security measures that could have prevented the breach of its data.

The Effect of the Data Breach on NBEO's Victims

44. The ramifications of NBEO's failure to protect the Personal Information of its exam-takers are severe. For example, the opening of a new credit card on its own is a significant credit event that requires a full credit inquiry on a consumer's credit report (known as a hard pull). A hard pull can result in the reduction of a consumer's credit score by up to five points. Thus, the fraudulent credit application alone can have a detrimental effect on a consumer's credit score.

45. In addition to adverse credit effects, Plaintiffs and class members have experienced numerous additional types of fraud. For instance:

a. An optometrist practicing in Illinois submitted her Personal Information to NBEO to sit for exams in 2011, 2012, 2013, and 2016. On August 28, 2016, she had a Chase Amazon Visa card opened in her name. On October 17, 2016, she had $11,213 withdrawn from her Chase savings account through three different transactions made at three different Chase banks in New York within 1.5 hours of each other. She closed that savings account and opened a new one on the same day. All of the money from her old savings (minus the $11,213 fraudulently withdrawn) was transferred into a new savings account. Despite setting up all the alerts, passwords, and notifications recommended by Chase, on October 19, 2016, $16,000 was transferred from her new savings account to her checking account by a phone transfer that she did not authorize. That same day she was forced to close both Chase accounts. Chase bank informed her that the fraudsters must have had a fake identification card made with her information on it, as well her Social Security number, to initiate the above transactions. On October 20, 2016, a Synchrony Bank card was opened in her name, and that same day a new Verizon iPhone line was added to her account. Also on October 20, 2016, fraudsters re-opened a closed Express Next card in her name in a store in Yonkers, New York and charged $1,059.25 to it. Additionally, on October 21, 2016, a Victoria's Secret card was opened in her name; on November 5, 2016, a Bloomingdale's credit card was applied for in her name; and on

November 7, 2016, a Saks Fifth Avenue credit card was applied for in her name, all without her authorization.

b. An optometrist practicing in Texas submitted her Personal Information to NBEO to sit for exams in 2002 and 2003. In September 2016, a Chase Amazon Visa credit card was fraudulently opened in her name. After realizing the scale of fraud affecting her fellow optometrists, she froze her credit with the three major credit reporting agencies. She has continued to contact Chase on a monthly basis to ensure that no other accounts have been fraudulently applied for in her name. Her credit score dropped because of the Chase inquiry and she still has not been able to get the inquiry off of her credit report. After hearing from other optometrists that many have had fraudulent PayPal accounts opened in their names, she has also called PayPal on a monthly basis to ensure no accounts have been opened. Having her credit frozen has caused a great deal of trouble because she was in the process of applying for a mortgage and has had to repeatedly unfreeze and refreeze her credit during the process. The Texas optometrist has spent countless hours requesting credit reports, changing passwords, and creating extra security measures on her email and bank accounts. After learning that some optometrists have had tax returns fraudulently filed using their stolen Personal Information, the optometrist spent time obtaining a PIN from the IRS in an attempt to keep fraudsters from filing a false return in her name. Additionally, at the beginning of April 2017, she learned of another attempt

> to open a fraudulent Chase Amazon Visa card in her name. Because her credit was frozen, the application was denied. She made multiple calls to Amazon and Chase to confirm the application was reported as fraudulent. Both Chase Amazon Visa cards were applied for using a Delaware address that she lived at for twelve months in 2004-2005. The only entity that had this address as well as her Social Security number was NBEO. In particular, she was applying for a Texas optometry license at this time and had to contact NBEO to request that her board scores be sent to the Texas Board of Optometry. She gave the Delaware address to NBEO at this time. In 12 years, she has had no communication with anyone using that Delaware address. It is a constant source of stress that she has built up excellent credit her entire life and someone out there has all of her Personal Information and can ruin that at any time they choose.

46. In addition to these examples and those of the named plaintiffs outlined above, thousands of additional class members have suffered significant and ongoing fraud in the wake of the NBEO breach.

47. Class members are also at risk of continuing fraud. Identity thieves can use the information taken in the breach to perpetrate a variety of crimes that harm victims. For instance, identity thieves may commit various types of government fraud such as immigration fraud, obtaining a driver's license or identification card in the victim's name but with another's picture, using the victim's information to obtain government benefits or medical care, or filing a fraudulent tax return using the victim's information to obtain a

fraudulent refund. Some of this activity may not come to light for years. Ongoing fraud has already manifested for numerous optometrists affected by this breach.

48. The U.S. Social Security Administration (SSA) warns that "[i]dentity theft is one of the fastest growing crimes in America."[8] The SSA has stated that "[i]dentity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought."[9] In short, "[s]omeone illegally using your Social Security number and assuming your identity can cause a lot of problems."[10]

49. Under SSA policy, individuals cannot obtain a new Social Security number until there is evidence of ongoing problems due to misuse of the Social Security number. Even then, the SSA recognizes that "a new number probably will not solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So using a new number will not guarantee you a fresh start."[11]

---

[8] *Identity Theft And Your Social Security Number*, *Social Security Administration* (Dec. 2013), http://www.ssa.gov/pubs/EN-05-10064.pdf (last visited July 5, 2017).

[9] *Id.*

[10] *Id.*

[11] *Id.*

50. In fact, a new Social Security number is substantially less effective where "other personal information, such as [the victim's] name and address, remains the same" and for some victims, "a new number actually creates new problems. If the old credit information is not associated with your new number, the absence of any credit history under your new number may make it more difficult for you to get credit."[12]

51. Identity thieves can use the victim's Personal Information to commit any number of frauds, such as obtaining a job, procuring housing, or even giving false information to police during an arrest. In the medical context, Personal Information can be used to submit false insurance claims, obtain prescription drugs or medical devices for black-market resale, or get medical treatment in the victim's name. As a result, Plaintiffs and class members now face a real and continuing immediate risk of identity theft and other problems associated with the disclosure of their Social Security numbers, and will need to monitor their credit and tax filings for an indefinite duration.

52. The processes of discovering and dealing with the repercussions of identity theft are time consuming and difficult. The Department of Justice's Bureau of Justice statistics found that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems."[13] Likewise, credit monitoring services are reactive not preventative, meaning they cannot catch identity theft until after it happens.

---

[12] *Id*.

[13] Erika Harrell and Lynn Langton, *Victims of Identity Theft, 2012*, (Bureau of Justice Statistics), Dec. 2013, http://www.bjs.gov/content/pub/pdf/vit12.pdf (last visited July 5, 2017).

53. Additionally, there is commonly lag time between when harm occurs and when it is discovered, and also between when Personal Information is stolen and when it is used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches: "law 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."[14]

54. There is a very strong probability that NBEO victims are at imminent risk of further fraud and identity theft for years into the future. Many class members report receiving an usually large number of emails designed to capture their personal information (known as "phishing"), and calls from unknown numbers where the caller hangs-up as soon as the class member answers the phone starting around the time the Chase Amazon Visa credit card applications began being filed.

55. As a result of NBEO's negligent security practices and delay in notifying affected individuals, Plaintiffs and other NBEO exam-takers now face years of constant monitoring of their financial and personal accounts and records to account for identity theft and fraud.

[14] U.S. Government Accountability Office, GAO Report to Congressional Requesters, *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, at 29, June 2007, http://www.gao.gov/new.items/d07737.pdf (last visited July 5, 2017).

56. Plaintiffs and members of the classes defined below have been harmed and are subject to an increased and concrete risk of further identity theft as a direct result of NBEO's exposure of their Personal Information.

CLASS ACTION ALLEGATIONS

57. Plaintiffs seek relief in their individual capacities and as representatives of all others who are similarly situated. Pursuant to Fed. R. Civ. P. 23(a), (b)(2), (b)(3), and/or (c)(4), Plaintiffs bring this action on behalf of themselves and the classes preliminarily defined as:

> All individuals who submitted their Personal Information to the NBEO and whose Personal Information was compromised as a result of the data breach discovered in or about July 2016 (the "Class").
>
> All residents of California who submitted their Personal Information to the NBEO and whose Personal Information was compromised as a result of the data breach discovered in or about July 2016 (the "California Subclass").
>
> All residents of New York who submitted their Personal Information to the NBEO and whose Personal Information was compromised as a result of the data breach discovered in or about July 2016 (the "New York Subclass").
>
> All residents of Missouri who submitted their Personal Information to the NBEO and whose Personal Information was compromised as a result of the data breach discovered in or about July 2016 (the "Missouri Subclass").
>
> All residents of New Jersey who submitted their Personal Information to the NBEO and whose Personal Information was compromised as a result of the data breach discovered in or about July 2016 (the "New Jersey Subclass").
>
> All residents of Illinois who submitted their Personal Information to the NBEO and whose Personal Information was compromised as a result of the data breach discovered in or about July 2016 (the "Illinois Subclass").
>
> All residents of Florida who submitted their Personal Information to the NBEO and whose Personal Information was compromised as a result of the data breach discovered in or about July 2016 (the "Florida Subclass").

> All residents of Texas who submitted their Personal Information to the NBEO and whose Personal Information was compromised as a result of the data breach discovered in or about July 2016 (the "Texas Subclass").
>
> All residents of Michigan who submitted their Personal Information to the NBEO and whose Personal Information was compromised as a result of the data breach discovered in or about July 2016 (the "Michigan Subclass").

58. Excluded from the classes are the NBEO, including any entity in which NBEO has a controlling interest, is a parent or subsidiary, or which is controlled by NBEO, as well as the officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns of NBEO. Also excluded are the judges and court personnel in this case and any members of their immediate families.

59. **Numerosity**. Fed. R. Civ. P. 23(a)(1). The members of the classes are so numerous that the joinder of all members is impractical. While the exact number of class members is unknown to Plaintiffs at this time, based on information and belief, it is in the thousands.

60. **Commonality**. Fed. R. Civ. P. 23(a)(2) and (b)(3). There are questions of law and fact common to the classes, which predominate over any questions affecting only individual class members. These common questions of law and fact include, without limitation:

a. Whether NBEO owed a duty to Plaintiffs and members of the classes to adequately protect their Personal Information and to provide timely and accurate notice of the data breach to Plaintiffs and members of the classes;

b. Whether NBEO knew or should have known that its systems were vulnerable to attack;

c. Whether NBEO's conduct, including its failure to act, resulted in or was the proximate cause of the breach of its systems, resulting in the loss of tens of thousands of individuals' Personal Information;

d. Whether Plaintiffs and members of the classes suffered injury, including ascertainable losses, as a result of NBEO's conduct or failure to act;

e. Whether NBEO's Personal Information storage and protection protocols were reasonable and compliant with industry standards;

f. Whether NBEO's conduct constituted unfair and deceptive trade practices actionable under the applicable consumer protection laws;

g. Whether NBEO's conduct violated data breach notification laws by failing to promptly notify class members that their Personal Information had been compromised;

h. Whether violated statutory obligations by failing to take all reasonable steps to dispose, or arrange for the disposal, of exam-takers' records within its custody or control containing Personal Information when the records should no longer have been retained by NBEO;

i. Whether Plaintiffs and members of the classes are entitled to recover actual damages and/or statutory damages; and

j. Whether Plaintiffs and members of the classes are entitled to equitable relief, including injunctive relief, restitution, and disgorgement.

61. All members of the proposed classes are readily ascertainable by objective criteria. NBEO has access to addresses and other contact information for members of the classes, which can be used for providing notice to many class members.

62. **Typicality**. Fed. R. Civ. P. 23(a)(3). Plaintiffs' claims are typical of those of other class members because Plaintiffs' Personal Information, like that of other class members, was misused and/or disclosed by NBEO.

63. **Adequacy of Representation**. Fed. R. Civ. P. 23(a)(4). Plaintiffs will fairly and adequately represent and protect the interests of the members of the classes. Plaintiffs' Counsel is competent and experienced in litigating class actions, including multiple class actions involving data breaches.

64. **Superiority of Class Action**. Fed. R. Civ. P. 23(b)(3). A class action is superior to other available methods for the fair and efficient adjudication of this controversy since joinder of all the members of the classes is impracticable. Furthermore, the adjudication of this controversy through a class action will avoid the possibility of inconsistent and potentially conflicting adjudication of the asserted claims. There will be no difficulty in the management of this action as a class action.

65. Damages for any individual class member are likely insufficient to justify the cost of individual litigation, so that in the absence of class treatment, NBEO's violations of law inflicting substantial damages in the aggregate would go likely un-remedied without certification of the classes.

66. Class certification is also appropriate under Fed. R. Civ. P. 23 because NBEO has acted or has refused to act on grounds generally applicable to the classes, so

that final injunctive relief or corresponding declaratory relief is appropriate as to the classes as a whole.

FIRST CAUSE OF ACTION
Negligence
(On Behalf of Plaintiffs and the Class)

67. Plaintiffs incorporate by reference all preceding paragraphs as if fully set forth herein.

68. Plaintiffs bring this cause of action on behalf of the Class.

69. In collecting the Personal Information of Plaintiffs and the Class, NBEO owed those individuals a duty to exercise reasonable care in safeguarding and protecting that information. This duty included, among other things, maintaining and testing NBEO's security systems and taking other reasonable security measures to protect and adequately secure the Personal Information of Plaintiffs and the Class from unauthorized access and use.

70. NBEO's security systems and procedures for handling the Personal Information of exam-takers and other individuals were intended to affect Plaintiffs and the Class. NBEO was aware that by gathering and storing such sensitive information, it had a responsibility to take reasonable security measures to protect the data from being stolen.

71. NBEO further had a duty to timely disclose to Plaintiffs and the Class that their Personal Information had been or was reasonably believed to have been compromised by NBEO and/or another person or entity acting under NBEO's control. Timely disclosure is appropriate so that Plaintiffs and the Class could, among other

things, report the theft of their Social Security numbers to the IRS, monitor their credit reports for identity fraud, obtain credit freezes, undertake appropriate measures to avoid unauthorized charges on their debit card or credit card accounts, and change or cancel their debit or credit card PINs (personal identification numbers) to prevent or mitigate the risk of fraudulent cash withdrawals or unauthorized transactions.

72. NBEO further had a duty to destroy the Personal Information of Plaintiffs and the Class from its databases within a reasonable amount of time after it was no longer necessary for NBEO to retain such information in order to mitigate the risk of loss of individuals' Personal Information in the event of a data breach.

73. NBEO breached its duty to exercise reasonable care in protecting the Personal Information of Plaintiffs and the Class by failing to implement and maintain adequate security measures to safeguard such information, failing to monitor its systems to identify suspicious activity, allowing unauthorized access to the Personal Information of Plaintiffs and the Class, and failing to adequately encrypt or otherwise prevent unauthorized access to such Personal Information.

74. NBEO further breached its duty to timely notify Plaintiffs and the Class about the data breach. NBEO has failed to issue adequate notice to individuals affected by the breach. Additionally, NBEO was, or should have been, aware of breaches in the network security of NBEO or a party acting under its control at least as early as August 1, 2016.

75. As a direct and proximate result of NBEO's failure to exercise reasonable care and use commercially reasonable security measures, the Personal Information of

Plaintiffs and the Class was accessed by unauthorized individuals who have used the information to commit identity theft and fraud. But for NBEO's failure to implement and maintain adequate security measures to protect individuals' Personal Information and failure to monitor its systems to identify suspicious activity, the Personal Information of Plaintiffs and Class would not have been stolen and used to open fraudulent lines of credit, and they would not be at a heightened risk of identity theft for years into the future.

76. Plaintiffs and the Class have also suffered economic damages, including the purchase of credit monitoring services they would not have otherwise purchased, and spent significant time addressing the effects of identity theft and fraud as well as taking preventative measure like notifying the IRS and credit reporting agencies.

77. Neither Plaintiffs nor members of the Class contributed to the security breach, nor did they contribute to NBEO's employment of insufficient security measures to safeguard individuals' stored Personal Information.

78. There is a causal connection between NBEO's failure to implement reasonable security measures to protect individuals' Personal Information and the injury to Plaintiffs and the Class. When individuals have their Personal Information stolen and used to apply for and/or open fraudulent accounts, they are at risk for additional identity theft, and are justified in purchasing credit monitoring services and other services to determine whether identity theft has or will occur.

79. NBEO is morally to blame for not protecting individuals' Personal Information by failing to take reasonable security measures. If NBEO had taken

reasonable security measures, data thieves would not have been able to take the Personal Information of thousands of current and former exam-takers and other individuals.

80. The policy of preventing future harm weighs in favor of finding a special relationship between NBEO and the Class. Exam-takers and other individuals who provide their Personal Information to NBEO rely on NBEO to keep their information safe and in fact are required to share sensitive personal data with NBEO as a condition of taking the optometry board exams necessary to practice optometry in the United States and Canada. If companies are not held accountable for failing to take reasonable security measures to protect their clients' Personal Information, then they will not take the steps that are necessary to protect against future cyber-attacks and data breaches.

81. It was foreseeable that if NBEO or its agents did not take reasonable security measures, the Personal Information of Plaintiffs and the Class would be stolen. Organizations like the NBEO face a high threat of security breaches due in part to the large amounts and type of information they store and the value of such information on the black market. NBEO should have known to take all reasonable precautions to secure individuals' Personal Information, especially in light of recent data breaches and publicity regarding cyberattacks.

82. NBEO's negligence was a substantial factor in causing harm to Plaintiffs and members of the class.

83. Plaintiffs and the class seek compensatory damages and punitive damages with interest, the costs of suit and attorneys' fees, and other and further relief as this Court deems just and proper.

SECOND CAUSE OF ACTION
Breach of Contract
(On Behalf of Plaintiffs and the Class)

84. Plaintiffs incorporate by reference all preceding paragraphs as if fully set forth herein.

85. Plaintiffs bring this cause of action on behalf of the Class.

86. NBEO's Privacy Statement promises that the company "has implemented a variety of encryption and security technologies and procedures to protect information stored in our computer systems from unauthorized access. We reveal only the last 4 digits of your credit card number when confirming orders as well as maintaining procedural safeguards that restrict your personal information to employees (or individuals working on our behalf and under confidentiality agreements) who need to know your personal information in order to provide products and/or services that you request." NBEO also purports to "use 128-bit [later changed to 256-bit] encryption technology and Secure Socket Layers ('SSL') in all areas where your personal and account information is required" and that its "Web site is certified by VeriSign, which verifies that [its] Web site is authentic and that [it] use[s] SSL security."[15]

87. NBEO's privacy policies constitute an agreement between NBEO and individuals who provided their Personal Information to NBEO.

88. NBEO has breached its agreement with Plaintiffs and the Class to protect their Personal Information by (1) failing to implement security measures designed to prevent this attack, (2) failing to employ security protocols to detect the unauthorized

[15] http://www.optometry.org/privacy.cfm.

network activity, and (3) failing to maintain basic security measures such as complex data encryption so that if data were accessed or stolen it would be unreadable.

89. Plaintiffs and the Class have been damaged by NBEO's breach of its contractual obligations because their Personal Information has been compromised and they have suffered identity theft and fraud, and/or are at an increased risk for identity theft and fraud. Plaintiffs and the Class have been deprived of the value of their Personal Information and have lost money and property as a result of NBEO's unlawful and unfair conduct.

90. Plaintiffs individually and on behalf of the Class seek recovery for damages suffered by members of the class, equitable relief, and injunctive relief requiring NBEO and its agents to implement safeguards consistent with its contractual promises.

THIRD CAUSE OF ACTION
Breach of Implied Contract
(On Behalf of Plaintiffs and the Class)

91. Plaintiffs incorporate by reference all preceding paragraphs as if fully set forth herein.

92. Plaintiffs bring this cause of action on behalf of the Class and to the extent necessary, in the alternative to their breach of contract claim.

93. When prospective optometrists and other consumers paid money and provided their Personal Information to NBEO in exchange for exam administration services, they entered into implied contracts with NBEO pursuant to which NBEO agreed to safeguard and protect such information and to timely and accurately notify them if their data had been breached and compromised.

94. NBEO solicited and invited prospective optometrists and other consumers to provide their Personal Information as part of its exam administration process. These individuals accepted NBEO's offers and provided their Personal Information to NBEO. In entering into such implied contracts, Plaintiffs and the Class assumed that NBEO's data security practices and policies were reasonable and consistent with industry standards, and that NBEO would use part of the funds received from Plaintiffs and the Class to pay for adequate and reasonable data security practices.

95. Plaintiffs and the Class would not have provided and entrusted their Personal Information to NBEO in the absence of the implied contract between them and NBEO to keep the information secure.

96. Plaintiffs and the Class fully performed their obligations under the implied contracts with NBEO.

97. NBEO breached its implied contracts with Plaintiffs and the Class by failing to safeguard and protect their Personal Information and by failing to provide timely and accurate notice that their Personal Information was compromised as a result of a data breach.

98. As a direct and proximate result of NBEO's breaches of the implied contracts, Plaintiffs and the Class sustained actual losses and damages as described herein.

FOURTH CAUSE OF ACTION
Unjust Enrichment
(On Behalf of Plaintiffs and the Class)

99. Plaintiffs incorporate by reference all preceding paragraphs as if fully set forth herein.

100. Plaintiffs allege in the alternative that they have no adequate remedy at law and bring this unjust enrichment claim on behalf of the Class.

101. Plaintiffs and the Class conferred a monetary benefit on NBEO in the form of fees paid to NBEO for exam administration services. Plaintiffs and the Class also provided their Personal Information to NBEO.

102. NBEO appreciated or had knowledge of the benefits conferred upon it by Plaintiffs and the Class.

103. The exam administration fees that Plaintiffs and the Class paid to NBEO should have been used by NBEO, in part, to pay for the costs of reasonable data privacy and security practices and procedures.

104. As a result of NBEO's conduct, Plaintiffs and the Class suffered actual damages in an amount equal to the difference in value between exam administration services with the reasonable data privacy and security practices and procedures that Plaintiffs and Class members paid for, and the inadequate exam administration services without reasonable data privacy and security practices and procedures that they received.

105. Under principles of equity and good conscience, NBEO should not be permitted to retain the money belonging to Plaintiffs and class members because NBEO

failed to implement (or adequately implement) the data privacy and security practices and procedures that Plaintiffs and class members paid for.

106. NBEO should be compelled to disgorge into a common fund for the benefit of Plaintiffs and the Class all unlawful or inequitable proceeds received by it.

107. A constructive trust should be imposed upon all unlawful or inequitable sums received by NBEO traceable to Plaintiffs and the Class.

FIFTH CAUSE OF ACTION
Violation of the Maryland Personal Information Protection Act and Consumer Protection Act, Maryland Code Commercial Law §§ 13-101 *et seq*., 14-3501 *et seq*.
(On Behalf of Plaintiffs and the Class)

108. Plaintiffs incorporate the above allegations by reference.

109. Plaintiffs bring this cause of action on behalf of the Class.

110. NBEO is incorporated in Maryland and subject to the laws of Maryland. Pursuant to the Maryland Personal Information Protection Act (PIPA), Maryland businesses have a statutory obligation to maintain the security of personal information of individuals.

111. "[T]o protect personal information from unauthorized access, use, modification, or disclosure," the Maryland Legislature enacted PIPA, Maryland Code, Commercial Law § 14-3503(a), which requires that any business that "owns or licenses personal information of an individual residing in the State shall implement and maintain reasonable security procedures and practices appropriate to the nature of the personal information owned or licensed and the nature and size of the business and its operations."

112. As described above, NBEO failed to implement and maintain reasonable security procedures and practices to protect the Personal Information of Plaintiffs and the Class, and thereby violated Maryland Code, Commercial Law § 14-3503(a).

113. The PIPA further provides that in the event of a security breach, notice must be given to consumers as soon as reasonably practicable following the investigation. The notice sent to consumer must include: a description of the information compromised; contact information for the business, including a toll-free number if the business has one; toll-free numbers and addresses for each of the three credit reporting agencies: Equifax, Experian and TransUnion; toll-free numbers, addresses and websites for the FTC and the Office of the Attorney General. *See* Maryland Code, Commercial Law § 14-3504.

114. Prior to sending notification to consumers, PIPA states that a business must notify the Office of the Attorney General that includes a brief description of the nature of the security breach, the number of Maryland residents being notified, what information has been compromised, and any steps the business is taking to restore the integrity of the system. *See id*.

115. As described above, NBEO has never notified affected individuals that NBEO or a party acting at its direction or under its control was subject to a data breach.

116. Under Maryland Code, Commercial Law section 14-3508, NBEO's violations of the PIPA also constitute unfair or deceptive trade practices prohibited by the Maryland Consumer Protection Act, and subject to the Consumer Protection Act's enforcement provisions.

117. Accordingly, NBEO is liable to Plaintiffs and the Class for damages and attorneys' fees under Maryland Code, Commercial Law § 13-408.

118. Plaintiffs and the Class seek all remedies available under Maryland law, including but not limited to, damages and attorneys' fees.

SIXTH CAUSE OF ACTION
Violation of the North Carolina Identity Theft Protection Act of 2005 and Unfair and Deceptive Trade Practices Act, N.C. Gen. Stat. §§ 75-65 *et seq*., 75-1.1 *et seq*.
(On Behalf of Plaintiffs and the Class)

119. Plaintiffs incorporate the above allegations by reference.

120. Plaintiffs bring this cause of action on behalf of the Class.

121. NBEO is incorporated in North Carolina and is subject to the laws of North Carolina. Pursuant to the North Carolina Identity Theft Protection Act Protection Act of 2005 ("IPA"), "[a]ny business that owns or licenses personal information of residents of North Carolina or any business that conducts business in North Carolina that owns or licenses personal information in any form (whether computerized, paper, or otherwise) shall provide notice to the affected person that there has been a security breach following discovery or notification of the breach." N.C. Gen. Stat. § 75-65(a).

122. The IPA provides that "[t]he disclosure notification shall be made without unreasonable delay . . . consistent with any measures necessary to determine sufficient contact information, determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system. For the purposes of this section, personal information shall not include electronic identification numbers, electronic mail names or addresses, Internet account numbers, Internet identification names, parent's

legal surname prior to marriage, or a password unless this information would permit access to a person's financial account or resources."

123. As described above, NBEO has never notified affected individuals that NBEO or a party acting at its direction or under its control was subject to a data breach.

124. Under IPA § 75-65(i), NBEO's willful failure to provide timely notice under the IPA is a violation of the North Carolina Unfair and Deceptive Trade Practices Act, N.C. Gen. Stat. § 75-1.1 *et seq.*, and subject to the Act's enforcement provisions.

125. Accordingly, Plaintiffs and the Class seek all remedies available under North Carolina law, including but not limited to, treble damages and attorneys' fees pursuant to N.C. Gen. Stat. §§ 75-16, 75-16.1.

SEVENTH CAUSE OF ACTION
Violation of the California Customer Records Act,
California Civil Code Section 1798.80, *et seq.*
(On Behalf of the California Subclass)

126. Plaintiffs incorporate by reference all preceding paragraphs as if fully set forth herein.

127. Plaintiff Fergason brings this cause of action on behalf of the California Subclass.

128. "[T]o ensure that personal information about California residents is protected," the California Legislature enacted Civil Code § 1798.81.5, which requires that any business that "owns or licenses personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to

the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."

129. NBEO is a "business" within the meaning of Civil Code § 1798.80(a).

130. Plaintiff Fergason and the California Subclass are "individual[s]" within the meaning of the Civil Code § 1798.80(d). Pursuant to Civil Code §§ 1798.80(e) and 1798.81.5(d)(1)(C), "personal information" includes an individual's name, Social Security number, driver's license or state identification card number, debit card and credit card information, medical information, or health insurance information. "Personal information" under Civil Code § 1798.80(e) also includes address, telephone number, passport number, education, employment, employment history, or health insurance information.

131. The breach of the Personal Information of the tens of thousands of NBEO exam-takers and other individuals constituted a "breach of the security system" of NBEO pursuant to Civil Code § 1798.82(g).

132. By failing to implement reasonable measures to protect the Personal Information of Plaintiff Fergason and the California Subclass, NBEO violated Civil Code § 1798.81.5.

133. In addition, by failing to take all reasonable steps to dispose, or arrange for the disposal, of exam-takers' and other individuals' records within its custody or control containing Personal Information when the records should no longer have been retained by NBEO, NBEO violated Civil Code § 1798.81.

134. In addition, by failing to promptly notify all affected individuals that their Personal Information had been acquired (or was reasonably believed to have been acquired) by unauthorized persons in the data breach, NBEO violated Civil Code § 1798.82 of the same title. NBEO's failure to timely notify affected individuals of the breach has caused damage to class members who have had to buy identity protection services or take other measures to remediate the effects of the breach.

135. By violating Civil Code §§ 1798.81.5, 1789.81 and 1798.82, NBEO "may be enjoined" under Civil Code § 1798.84(e).

136. Accordingly, Plaintiff Fergason requests that the Court enter an injunction requiring NBEO to implement and maintain reasonable security procedures to protect exam-takers' and other individuals' Personal Information in compliance with the California Customer Records Act, including, but not limited to: (1) ordering that NBEO, consistent with industry standard practices, engage third party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on NBEO's systems on a periodic basis; (2) ordering that NBEO engage third party security auditors and internal personnel, consistent with industry standard practices, to run automated security monitoring; (3) ordering that NBEO audit, test, and train its security personnel regarding any new or modified procedures; (4) ordering that NBEO, consistent with industry standard practices, conduct regular database scanning and security checks; (5) ordering that NBEO, consistent with industry standard practices, periodically conduct internal training and education to inform internal security personnel how to identify and contain a

breach when it occurs and what to do in response to a breach; (6) ordering NBEO to meaningfully educate affected individuals about the threats they face as a result of the loss of their Personal Information to third parties, as well as the steps they must take to protect themselves; and (7) ordering NBEO to adequately encrypt sensitive personal information.

137. Plaintiffs further request that the Court require NBEO to (1) identify and notify all members of the California Subclass regarding the existence and effects of the data breach; and (2) to notify affected individuals of any future data breaches by email within 24 hours of NBEO's discovery of a breach or possible breach and by mail within 72 hours.

138. As a result of NBEO's violation of Civil Code §§ 1798.81.5, 1798.81 and 1798.82, Plaintiffs and the California Subclass have and will incur economic damages relating to time and money spent remedying the breach, including but not limited to, expenses for bank fees associated with the breach, any unauthorized charges made on financial accounts, lack of access to funds while banks issue new cards, tax fraud, as well as the costs of credit monitoring and purchasing credit reports.

139. Plaintiffs, individually and on behalf of the members of the California Subclass, seek all remedies available under Civil Code § 1798.84, including, but not limited to damages suffered by members of the class and equitable relief.

140. Plaintiffs, individually and on behalf of the members of the California Subclass, seek reasonable attorneys' fees and costs under applicable law.

EIGHTH CAUSE OF ACTION
Unlawful and Unfair Business Practices Under California Business and Professions Code § 17200, *et seq.*
(On Behalf of the California Subclass)

141. Plaintiffs incorporate by reference all preceding paragraphs as if fully set forth herein.

142. Plaintiff Fergason brings this cause of action on behalf of the California Subclass.

143. NBEO's acts and practices, as alleged in this Complaint, constitute unlawful and unfair business practices, in violation of the Unfair Competition Law ("UCL"), Cal. Bus. & Prof. Code § 17200, *et seq*., and because NBEO's conduct was negligent:

a. NBEO's practices were unlawful and in violation of California Civil Code § 1798.81.5(b) because NBEO failed to take reasonable security measures in protecting individuals' Personal Information;

b. NBEO's practices were unlawful and in violation of California Civil Code § 1798.81 because NBEO failed to take all reasonable steps to dispose, or arrange for the disposal, of individuals' records within its custody or control containing Personal Information when the records should no longer have been retained by NBEO;

c. NBEO's practices were unlawful and in violation of California Civil Code § 1798.82 because NBEO has unreasonably delayed informing Plaintiffs and the California Subclass about the breach of security after NBEO knew the data

breach occurred; and

d. NBEO's practices were unlawful and in violation of Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45(a) because NBEO adopted unreasonable data security practices that constitute unfair and deceptive acts and practices in and affecting commerce.

144. The acts, omissions, and conduct of NBEO constitute a violation of the unlawful prong of the UCL because NBEO failed to comport with a reasonable standard of care and California public policy as reflected in statutes such as the Information Practices Act of 1977, Cal. Civ. Code § 1798, *et seq.*, and California Customer Records Act, which seek to protect individuals' data and ensure that entities who solicit or are entrusted with personal data utilize reasonable security measures.

145. In failing to protect exam takers' Personal Information and unduly delaying informing them of the data breach, NBEO has engaged in unfair business practices by engaging in conduct that undermines or violates the stated policies underlying the California Customer Records Act and the Information Practices Act of 1977. In enacting the California Customer Records Act, the Legislature stated that: "[i]dentity theft is costly to the marketplace and to consumers" and that "victims of identity theft must act quickly to minimize the damage; therefore expeditious notification of possible misuse of a person's personal information is imperative." 2002 Cal. Legis. Serv. Ch. 1054 (A.B. 700). NBEO's conduct also undermines California public policy as reflected in other statutes such as the Information Practices Act of 1977, Cal. Civ. Code § 1798, *et seq.*,

which seeks to protect individuals' data and ensure that entities who solicit or are entrusted with personal data utilize reasonable security measures.

146. As a direct and proximate result of NBEO's unlawful and unfair business practices as alleged herein, Plaintiffs and the California Subclass have suffered injury in fact. Plaintiffs and the California Subclass have been injured in that their Personal Information has been compromised and used to conduct identity theft and fraud, and they are at an increased risk for additional future identity theft and fraud. Plaintiffs and the California Subclass have also lost money and property mitigating the effects of the breach by purchasing credit monitoring and other services they would not otherwise had to but for NBEO's unlawful and unfair conduct.

147. As a direct and proximate result of NBEO's unlawful and unfair business practices as alleged herein, Plaintiffs and the California Subclass face continued identity and theft and an increased risk of future identity theft based on the theft and disclosure of their Personal Information.

148. Because of NBEO's unfair and unlawful business practices, Plaintiffs and the California Subclass are entitled to relief, including restitution for costs incurred associated with the data breach and disgorgement of all profits accruing to NBEO because of its unlawful and unfair business practices, declaratory relief, and a permanent injunction enjoining NBEO from its unlawful and unfair practices.

149. The injunctive relief that Plaintiffs and the California Subclass are entitled to includes, but is not limited to: (1) ordering that NBEO, consistent with industry standard practices, engage third party security auditors/penetration testers as well as

internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on NBEO's systems on a periodic basis; (2) ordering that NBEO engage third party security auditors and internal personnel, consistent with industry standard practices, to run automated security monitoring; (3) ordering that NBEO audit, test, and train its security personnel regarding any new or modified procedures; (4) ordering that NBEO, consistent with industry standard practices, conduct regular database scanning and security checks; (5) ordering that NBEO, consistent with industry standard practices, periodically conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; (6) ordering NBEO to meaningfully educate affected individuals about the threats they face as a result of the loss of their personal information to third parties, as well as the steps they must take to protect themselves; and (7) ordering NBEO to adequately encrypt sensitive personal information.

150. Plaintiffs, individually and on behalf of the members of the California Subclass, also seeks reasonable attorneys' fees and costs under applicable law.

NINTH CAUSE OF ACTION
Violation of New York General Business Law, N.Y. Gen. Bus. Law § 349, *et seq*.
(On Behalf of the New York Subclass)

151. Plaintiffs incorporate the above allegations by reference.

152. Plaintiff Liang brings this cause of action on behalf of the New York Subclass.

153. NBEO engaged in deceptive, unfair, and unlawful trade acts or practices in the conduct of trade or commerce and furnishing of consumer-oriented services, in violation of N.Y. Gen. Bus. Law § 349(a), including but not limited to the following:

a. NBEO misrepresented and fraudulently advertised material facts, pertaining to the sale, furnishing and/or registration for exam administration services, to the New York Subclass by representing and advertising that they would maintain adequate data privacy and security practices and procedures to safeguard New York Subclass members' Personal Information from unauthorized disclosure, release, data breaches, and theft;

b. NBEO misrepresented material facts, pertaining to sale and/or furnishing of optometry exam services, to the New York Subclass by representing and advertising that they did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of New York Subclass members' Personal Information;

c. NBEO omitted, suppressed, and concealed the material fact of the inadequacy of their privacy and security protections for New York Subclass members' Personal Information;

d. NBEO engaged in deceptive, unfair, and unlawful trade acts or practices by failing to maintain the privacy and security of New York Subclass members' Personal Information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the NBEO data breach. These unfair acts and practices violated duties imposed by state and

federal laws, including section 5 of the Federal Trade Commission Act (15 U.S.C. § 45);

e. NBEO engaged in deceptive, unfair, and unlawful trade acts or practices by failing to disclose the NBEO data breach to New York Subclass members in a timely and accurate manner, contrary to the duties imposed by N.Y. Gen Bus. Law § 899-aa(2);

f. NBEO engaged in deceptive, unfair, and unlawful trade acts or practices by failing to take proper action following the NBEO data breach to enact adequate privacy and security measures and protect New York Subclass members' Personal Information from further unauthorized disclosure, release, data breaches, and theft.

154. As a direct and proximate result of NBEO's deceptive trade practices, New York Subclass members suffered injury and/or damages, including the loss of their legally protected interest in the confidentiality and privacy of their Personal Information, and the loss of the benefit of their bargain.

155. The above unfair and deceptive practices and acts by NBEO were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to consumers that these consumers could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

156. NBEO knew or should have known that its computer systems and data security practices were inadequate to safeguard New York Subclass members' Personal Information and that risk of a data breach or theft was highly likely. NBEO's actions in

engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the New York Subclass.

157. Plaintiff and the New York Subclass seek relief under N.Y. Gen. Bus. Law § 349(h), including, but not limited to, actual damages, treble damages, statutory damages, injunctive relief, and/or attorney's fees and costs.

TENTH CAUSE OF ACTION
Violation of Missouri Merchandising Practices Act, Mo. Rev. Stat. § 407.010, *et seq*., (On Behalf of the Missouri Subclass)

158. Plaintiffs incorporate the above allegations by reference.

159. Plaintiff Olendorff brings this cause of action on behalf of the Missouri Subclass.

160. In paying for exam administration services offered by NBEO, members of the Missouri Subclass purchased "merchandise" in trade or commerce for personal, family, and/or household purposes within the meaning of Mo. Rev. Stat. § 407.010.

161. NBEO engaged in unlawful, unfair, and deceptive acts and practices, misrepresentation, and the concealment, suppression, and omission of material facts with respect to the sale and advertisement of the services in violation of Mo. Rev. Stat. § 407.020(1), including but not limited to the following:

a. NBEO misrepresented and fraudulently advertised material facts, pertaining to the sale, furnishing and/or registration for exam administration services, to the Missouri Subclass by representing and advertising that they would maintain adequate data privacy and security practices and procedures to

safeguard Missouri Subclass members' Personal Information from unauthorized disclosure, release, data breaches, and theft;

b. NBEO misrepresented material facts, pertaining to sale and/or furnishing of optometry exam services, to the Missouri Subclass by representing and advertising that they did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Missouri Subclass members' Personal Information;

c. NBEO omitted, suppressed, and concealed the material fact of the inadequacy of their privacy and security protections for Missouri Subclass members' Personal Information;

d. NBEO engaged in deceptive, unfair, and unlawful trade acts or practices by failing to maintain the privacy and security of Missouri Subclass members' Personal Information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the NBEO data breach. These unfair acts and practices violated duties imposed by state and federal laws, including section 5 of the Federal Trade Commission Act (15 U.S.C. § 45);

e. NBEO engaged in deceptive, unfair, and unlawful trade acts or practices by failing to disclose the NBEO data breach to Missouri Subclass members in a timely and accurate manner, in violation of Mo. Rev. Stat. § 407.1500(2)(1)(a);

f. NBEO engaged in deceptive, unfair, and unlawful trade acts or practices by failing to take proper action following the NBEO data breach to enact adequate privacy and security measures and protect Missouri Subclass members' Personal Information from further unauthorized disclosure, release, data breaches, and theft.

162. The above unlawful and deceptive acts and practices and acts by NBEO were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to consumers that the consumers could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

163. NBEO knew or should have known that their computer systems and data security practices were inadequate to safeguard Missouri Subclass members' Personal Information and that risk of a data breach or theft was highly likely. NBEO's actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the Missouri Subclass.

164. As a direct and proximate result of NBEO's unlawful practices, members of the Missouri Subclass suffered an ascertainable loss of money or property, real or personal, as described above, including the loss of their legally protected interest in the confidentiality and privacy of their Personal Information.

165. Missouri Subclass members seek relief under Mo. Rev. Stat. § 407.025, including, but not limited to, injunctive relief, actual damages, punitive damages, and attorneys' fees and costs.

ELEVENTH CAUSE OF ACTION
Violation of the New Jersey Consumer Fraud Act, N.J. Stat. Ann. § 56:8-1, *et seq*.,
(On Behalf of the New Jersey Subclass)

166. Plaintiffs incorporate the above allegations by reference.

167. Plaintiff Robinson brings this cause of action on behalf of the New Jersey Subclass.

168. NBEO sells merchandise within the meaning of N.J. Stat. Ann. § 56:8-1 by offering exam administration services to members of the public.

169. NBEO engaged in unconscionable and deceptive acts and practices, misrepresentation, and the concealment, suppression, and omission of material facts with respect to the sale and advertisement of services in violation of N.J. Stat. Ann. § 56:8-2, including but not limited to the following:

a. NBEO misrepresented and fraudulently advertised material facts, pertaining to the sale, furnishing and/or registration for exam administration services, to the New Jersey Subclass by representing and advertising that they would maintain adequate data privacy and security practices and procedures to safeguard New Jersey Subclass members' Personal Information from unauthorized disclosure, release, data breaches, and theft;

b. NBEO misrepresented material facts, pertaining to sale and/or furnishing of optometry exam services, to the New Jersey Subclass by representing and advertising that they did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of New Jersey Subclass members' Personal Information;

c. NBEO omitted, suppressed, and concealed the material fact of the inadequacy of their privacy and security protections for New Jersey Subclass members' Personal Information;

d. NBEO engaged in deceptive, unfair, and unlawful trade acts or practices by failing to maintain the privacy and security of New Jersey Subclass members' Personal Information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the NBEO data breach. These unfair acts and practices violated duties imposed by state and federal laws, including section 5 of the Federal Trade Commission Act (15 U.S.C. § 45);

e. NBEO engaged in deceptive, unfair, and unlawful trade acts or practices by failing to disclose the NBEO data breach to New Jersey Subclass members in a timely and accurate manner, in violation of N.J. Stat. Ann. § 56:8-163(a);

f. NBEO engaged in deceptive, unfair, and unlawful trade acts or practices by failing to take proper action following the NBEO data breach to enact adequate privacy and security measures and protect New Jersey Subclass members' Personal Information from further unauthorized disclosure, release, data breaches, and theft.

170. The above unlawful and deceptive acts and practices and acts by NBEO were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial

injury to consumers that the consumers could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

171. NBEO knew or should have known that their computer systems and data security practices were inadequate to safeguard New Jersey Subclass members' Personal Information and that risk of a data breach or theft was highly likely. NBEO's actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the New Jersey Subclass.

172. As a direct and proximate result of NBEO's unconscionable or deceptive acts and practices, New Jersey Subclass 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 Personal Information.

173. Members of the New Jersey Subclass seek relief under N.J. Stat. Ann. § 56:8-19, including, but not limited to, injunctive relief, other equitable relief, actual damages, treble damages, and attorneys' fees and costs.

TWELFTH CAUSE OF ACTION
Violation of the Illinois Consumer Fraud Act, 815 Ill. Comp. Stat. 505/1, *et seq.*,
(On Behalf of the Illinois Subclass)

174. Plaintiffs incorporate the above allegations by reference.

175. Plaintiff Pappas-Walker brings this cause of action on behalf of the Illinois Subclass.

176. NBEO engaged in deceptive, unfair, and unlawful trade acts or practices in the conduct of trade or commerce, in violation of 815 Ill. Comp. Stat. 505/2, including but not limited to the following:

a. NBEO misrepresented and fraudulently advertised material facts, pertaining to the sale, furnishing and/or registration for exam administration services, to the Illinois Subclass by representing and advertising that they would maintain adequate data privacy and security practices and procedures to safeguard Illinois Subclass members' Personal Information from unauthorized disclosure, release, data breaches, and theft;

b. NBEO misrepresented material facts, pertaining to sale and/or furnishing of optometry exam services, to the Illinois Subclass by representing and advertising that they did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Illinois Subclass members' Personal Information;

c. NBEO omitted, suppressed, and concealed the material fact of the inadequacy of their privacy and security protections for Illinois Subclass members' Personal Information;

d. NBEO engaged in deceptive, unfair, and unlawful trade acts or practices by failing to maintain the privacy and security of Illinois Subclass members' Personal Information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the NBEO data breach. These unfair acts and practices violated duties imposed by state and

federal laws, including section 5 of the Federal Trade Commission Act (15 U.S.C. § 45);

e. NBEO engaged in deceptive, unfair, and unlawful trade acts or practices by failing to disclose the NBEO data breach to Illinois Subclass members in a timely and accurate manner, contrary to the duties imposed by 815 Ill. Comp. Stat. § 530/10(a);

f. NBEO engaged in deceptive, unfair, and unlawful trade acts or practices by failing to take proper action following the NBEO data breach to enact adequate privacy and security measures and protect Illinois Subclass members' Personal Information from further unauthorized disclosure, release, data breaches, and theft.

177. As a direct and proximate result of NBEO's deceptive trade practices, Illinois Subclass members suffered injuries, including the loss of their legally protected interest in the confidentiality and privacy of their Personal Information, and damages, as described above.

178. The above unfair and deceptive practices and acts by NBEO were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury that these consumers could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

179. NBEO knew or should have known that their computer systems and data security practices were inadequate to safeguard Illinois Subclass members' Personal Information and that risk of a data breach or theft was highly likely. NBEO's actions in

engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the Illinois Subclass.

180. Illinois Subclass members seek relief under 815 Ill. Comp. Stat. 505/10a, including, but not limited to, damages, restitution, punitive damages, injunctive relief, and/or attorneys' fees and costs.

THIRTEENTH CAUSE OF ACTION
Violation of Illinois Uniform Deceptive Trade Practices Act,
815 Ill. Comp. Stat. § 510/2(a), *et seq*.,
(On Behalf of the Illinois Subclass)

181. Plaintiffs incorporate the above allegations by reference.

182. Plaintiff Pappas-Walker brings this cause of action on behalf of the Illinois Subclass.

183. While in the course of their business, NBEO engaged in deceptive trade practices by making false representations, including their representations that it had adequate computer systems and data security practices to protect Personal Information, when their computer systems and data security practices were inadequate, in violation of 815 Ill. Comp. Stat. 510/2(a)(5),(7).

184. NBEO knew or should have known that it or someone acting under its control had inadequate data security practices and engaged in acts that were negligent, knowing, and/or willful acts of deception.

185. Illinois Subclass members are likely to be damaged by NBEO's deceptive trade practices.

186. Illinois Subclass members seek relief under 815 Ill. Comp. Stat. 510, including, but not limited to, injunctive relief and attorneys' fees.

FOURTEENTH CAUSE OF ACTION
Violation of the Florida Deceptive and Unfair Trade Practices Act, Fla. Stat. Ann. § 501.204(1), *et seq*.
(On Behalf of the Florida Subclass)

187. Plaintiffs incorporate the above allegations by reference.

188. Plaintiffs Wolf and Dunn bring this cause of action on behalf of the Florida Subclass.

189. Florida Subclass members purchased merchandise and services in trade or commerce when they paid for exam administration services offered by NBEO for personal, family, and/or household purposes.

190. NBEO engaged in unlawful, unfair, and deceptive acts and practices, misrepresentation, and the concealment, suppression, and omission of material facts with respect to the sale and advertisement of the services in violation of Fla. Stat. Ann. § 501.204(1), including but not limited to the following:

a. NBEO misrepresented and fraudulently advertised material facts, pertaining to the sale, furnishing and/or registration for exam administration services, to the Florida Subclass by representing and advertising that they would maintain adequate data privacy and security practices and procedures to safeguard Florida Subclass members' Personal Information from unauthorized disclosure, release, data breaches, and theft;

b. NBEO misrepresented material facts, pertaining to sale and/or furnishing of optometry exam services, to the Florida Subclass by representing and advertising that they did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Florida Subclass members' Personal Information;

c. NBEO omitted, suppressed, and concealed the material fact of the inadequacy of their privacy and security protections for Florida Subclass members' Personal Information;

d. NBEO engaged in deceptive, unfair, and unlawful trade acts or practices by failing to maintain the privacy and security of Florida Subclass members' Personal Information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the NBEO data breach. These unfair acts and practices violated duties imposed by state and federal laws, including section 5 of the Federal Trade Commission Act (15 U.S.C. § 45);

e. NBEO engaged in deceptive, unfair, and unlawful trade acts or practices by failing to disclose the NBEO data breach to Florida Subclass members in a timely and accurate manner, in violation of Fla. Stat. Ann. § 501.171;

f. NBEO engaged in deceptive, unfair, and unlawful trade acts or practices by failing to take proper action following the NBEO data breach to enact adequate privacy and security measures and protect Florida Subclass

members' Personal Information from further unauthorized disclosure, release, data breaches, and theft.

191. The above unlawful and deceptive acts and practices and acts by NBEO were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to consumers that the consumers could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

192. NBEO knew or should have known that their computer systems and data security practices were inadequate to safeguard Florida Subclass members' Personal Information and that risk of a data breach or theft was highly likely. NBEO's actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the Florida Class.

193. As a direct and proximate result of NBEO's unlawful practices, Florida Subclass members suffered an ascertainable loss of money or property, real or personal, as described above, including the loss of their legally protected interest in the confidentiality and privacy of their Personal Information.

194. Florida Subclass members seek relief under relief under Fla. Stat. Ann. § 501.211, including, but not limited to, injunctive relief, actual damages, punitive damages, and attorneys' fees and costs.

FIFTEENTH CAUSE OF ACTION
Violation of the Texas Deceptive Trade Practices-Consumer Protection Act, Tex. Bus. & Com. Code §§ 17.41, *et seq*.
(On Behalf of the Florida Subclass)

195. Plaintiffs incorporate the above allegations by reference.

196. Plaintiff Nelson brings this cause of action on behalf of the Texas Subclass.

197. NBEO engaged in unlawful, unfair, and deceptive acts and practices, misrepresentation, and the concealment, suppression, and omission of material facts with respect to the sale and advertisement of the services in violation of Tex. Bus. & Com. Code § 17.46(b), including but not limited to the following:

a. NBEO misrepresented and fraudulently advertised material facts, pertaining to the sale, furnishing and/or registration for exam administration services, to the Texas Subclass by representing and advertising that they would maintain adequate data privacy and security practices and procedures to safeguard Texas Subclass members' Personal Information from unauthorized disclosure, release, data breaches, and theft;

b. NBEO misrepresented material facts, pertaining to sale and/or furnishing of optometry exam services, to the Texas Subclass by representing and advertising that they did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Texas Subclass members' Personal Information;

c. NBEO omitted, suppressed, and concealed the material fact of the inadequacy of their privacy and security protections for Texas Subclass members' Personal Information;

d. NBEO engaged in deceptive, unfair, and unlawful trade acts or practices by failing to maintain the privacy and security of Texas Subclass members' Personal Information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the NBEO data breach. These unfair acts and practices violated duties imposed by state and federal laws, including section 5 of the Federal Trade Commission Act (15 U.S.C. § 45);

e. NBEO engaged in deceptive, unfair, and unlawful trade acts or practices by failing to disclose the NBEO data breach to Texas Subclass members in a timely and accurate manner, in violation of Tex. Bus. & Com. Code § 521.053;

f. NBEO engaged in deceptive, unfair, and unlawful trade acts or practices by failing to take proper action following the NBEO data breach to enact adequate privacy and security measures and protect Texas Subclass members' Personal Information from further unauthorized disclosure, release, data breaches, and theft.

198. The above unlawful and deceptive acts and practices and acts by NBEO were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial

injury to consumers that the consumers could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

199. NBEO knew or should have known that their computer systems and data security practices were inadequate to safeguard Texas Subclass members' Personal Information and that risk of a data breach or theft was highly likely. NBEO's actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the Texas Subclass.

200. As a direct and proximate result of NBEO's unlawful practices, Texas Subclass members suffered an ascertainable loss of money or property, real or personal, as described above, including the loss of their legally protected interest in the confidentiality and privacy of their Personal Information. On September 28, 2016, Plaintiffs provided NBEO with a pre-suit demand letter pursuant to Tex. Bus. & Com. Code § 17.505(a) and Cal. Civ. Code § 1782(a).

201. Texas Subclass members seek relief under relief under Tex. Bus. & Com. Code § 17.505, including, but not limited to, injunctive relief, actual damages, punitive damages, and attorneys' fees and costs.

SIXTEENTH CAUSE OF ACTION
Violation of the Michigan Consumer Protection Act,
Mich. Comp. Laws § 445.901, *et seq*.
(On Behalf of the Michigan Subclass)

202. Plaintiffs incorporate the above allegations by reference.

203. Plaintiff Garin brings this cause of action on behalf of the Michigan Subclass.

204. NBEO engaged in unlawful, unfair, and deceptive acts and practices, misrepresentation, and the concealment, suppression, and omission of material facts with respect to the sale and advertisement of the services in violation of Mich. Comp. Laws § 445.903, including but not limited to the following:

a. NBEO misrepresented and fraudulently advertised material facts, pertaining to the sale, furnishing and/or registration for exam administration services, to the Michigan Subclass by representing and advertising that they would maintain adequate data privacy and security practices and procedures to safeguard Michigan Subclass members' Personal Information from unauthorized disclosure, release, data breaches, and theft;

b. NBEO misrepresented material facts, pertaining to sale and/or furnishing of optometry exam services, to the Michigan Subclass by representing and advertising that they did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Michigan Subclass members' Personal Information;

c. NBEO omitted, suppressed, and concealed the material fact of the inadequacy of their privacy and security protections for Michigan Subclass members' Personal Information;

d. NBEO engaged in deceptive, unfair, and unlawful trade acts or practices by failing to maintain the privacy and security of Michigan Subclass members'

Personal Information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the NBEO data breach. These unfair acts and practices violated duties imposed by state and federal laws, including section 5 of the Federal Trade Commission Act (15 U.S.C. § 45);

e. NBEO engaged in deceptive, unfair, and unlawful trade acts or practices by failing to disclose the NBEO data breach to Michigan Subclass members in a timely and accurate manner, in violation of Mich. Comp. Laws Ann. § 445.72;

f. NBEO engaged in deceptive, unfair, and unlawful trade acts or practices by failing to take proper action following the NBEO data breach to enact adequate privacy and security measures and protect Michigan Subclass members' Personal Information from further unauthorized disclosure, release, data breaches, and theft.

205. The above unlawful and deceptive acts and practices and acts by NBEO were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to consumers that the consumers could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

206. NBEO knew or should have known that their computer systems and data security practices were inadequate to safeguard Michigan Subclass members' Personal Information and that risk of a data breach or theft was highly likely. NBEO's actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing

and willful, and/or wanton and reckless with respect to the rights of members of the Michigan Subclass.

207. As a direct and proximate result of NBEO's unlawful practices, Michigan Subclass members suffered an ascertainable loss of money or property, real or personal, as described above, including the loss of their legally protected interest in the confidentiality and privacy of their Personal Information.

208. Michigan Subclass members seek relief under relief under Mich. Comp. Laws § 445.910, including, but not limited to, injunctive relief, actual damages, punitive damages, and attorneys' fees and costs.

SEVENTEENTH CAUSE OF ACTION
Violations of State Data Breach Notification Statutes
(On Behalf of the California, Illinois, Texas, Michigan, and New Jersey Subclasses)

209. Plaintiffs incorporate the above allegations by reference.

210. Legislatures in the states and jurisdictions listed below have enacted data breach statutes that provide consumers with a private cause of action. These statutes generally apply to any person or business conducting business within the state that owns or licenses computerized data containing personal information. If the personal information is acquired or accessed in a way that compromises its security or confidentiality, the covered entity must notify the affected individuals in the most expedient time and manner possible and without unreasonable delay.

211. The NBEO data breach constituted a security breach that triggered the notice provisions of the data breach statutes and the Personal Information taken includes categories of personal information protected by the data breach statutes.

212. Despite conducting an "investigation," NBEO has not informed affected individuals that NBEO or a party acting under its control had a data security breach after NBEO knew or should have known that the data breach had occurred.

213. Plaintiffs and members of the California, Illinois, Texas, Michigan, and New Jersey Subclasses were damaged by NBEO's failure to comply with the data breach statutes.

214. Had NBEO provided timely and accurate notice, Plaintiffs and members of the California, Illinois, Texas, Michigan, and New Jersey Subclasses could have avoided or mitigated the harm caused by the data breach. For example, they could have contacted their financial institutions, placed credit freezes and fraud alerts on their credit accounts, reported possible fraud to the IRS, purchased credit monitoring, and taken security precautions in time to prevent or minimize identity theft.

215. NBEO's failure to provide timely and accurate notice of the NBEO data breach violated the following state data breach statutes:

a. Cal. Civ. Code § 1798.80, *et seq.*;

b. Ill. Comp. Stat. Ann. 530/10(a), *et seq.*;

c. Tex. Bus. & Com. Code § 521.053, *et seq.*;

d. Mich. Comp. Laws Ann. § 445.72(1), *et seq.*; and

e. N.J. Stat. Ann. § 56:8-163(a), *et seq.*

216. Plaintiffs and members of the California, Illinois, Texas, Michigan, and New Jersey Subclasses seek all remedies available under their respective state data breach statutes, including but not limited to damages, equitable relief, including

injunctive relief, damages, reasonable attorneys' fees and costs, as provided by the applicable laws.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and the classes set forth herein, respectfully requests the following relief:

a. That the Court certify this case as a class action pursuant to Fed. R. Civ. P. 23(a), (b)(2), (b)(3), and/or (c)(4), pursuant to Fed. R. Civ. P. 23(g), appoint the named Plaintiffs to be Class representatives and the undersigned counsel to be Class counsel;

b. That the Court award Plaintiffs and the classes appropriate relief, including actual and statutory damages, restitution and disgorgement;

c. That the Court award Plaintiffs and the classes equitable, injunctive and declaratory relief as may be appropriate under applicable state laws;

d. That the Court award Plaintiffs and the classes actual damages, compensatory damages, statutory damages, and statutory penalties, to the full extent permitted by law, in an amount to be determined;

e. That the Court award Plaintiffs and the classes pre-judgment and post-judgment interest;

f. That the Court award Plaintiffs and the classes reasonable attorneys' fees and costs as allowable by law; and

g. That the Court award Plaintiffs and the classes such other, favorable relief as allowable under law or at equity.

JURY DEMAND

Plaintiffs hereby demand a jury trial in the instant action.

Dated: July 14, 2017

Respectfully submitted,

By: /s/ Hassan Zavareei

Hassan Zavareei (No. 18489)
TYCKO & ZAVAREEI LLP
1828 L. Street, NW, Suite 1000
Washington, DC 20036
hzavareei@tzlegal.com
Tel: (202) 973-0910
Fax: (202) 973-0950

Norman E. Siegel
Barrett J. Vahle
J. Austin Moore
STUEVE SIEGEL HANSON LLP
460 Nichols Road, Suite 200
Kansas City MO 64112
siegel@stuevesiegel.com
vahle@stuevesiegel.com
moore@stuevesiegel.com
Tel: (816) 714-7100
Fax: (816) 714-7101

Michael Liskow
WOLF HALDENSTEIN ADLER
FREEMAN AND HERZ LLP
270 Madison Ave
New York, NY 10016
Tel: (212) 545-4600
Fax: (212) 545-4653
liskow@whafh.com

Carl Malmstrom
WOLF HALDENSTEIN ADLER
FREEMAN AND HERZ LLC
One South Dearborn St., Suite 2122
Chicago, IL 60603
Tel: (312) 984-0000
Fax: (312) 212-4401
malmstrom@whafh.com

Counsel for Plaintiffs and the Class