BLOOD HURST & O'REARDON, LLP
TIMOTHY G. BLOOD (149343)
PAULA M. ROACH (254142)
701 B Street, Suite 1700
San Diego, CA 92101
Tel: 619/338-1100
619/338-1101 (fax)
tblood@bholaw.com
proach@bholaw.com

BARNOW AND ASSOCIATES, P.C.
BEN BARNOW
ERICH P. SCHORK
1 North LaSalle Street, Suite 4600
Chicago, IL 60602
Tel: 312/621-2000
312/641-5504 (fax)
b.barnow@barnowlaw.com
e.schork@barnowlaw.com

THE COFFMAN LAW FIRM
RICHARD L. COFFMAN
First City Building
505 Orleans St., Suite 505
Beaumont, TX 77701
Tel: 409/833-7700
866/835-8250 (fax)
rcoffman@coffmanlawfirm.com

Attornevs for Plaintiffs and the Putative Class

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

MAUDIE PATTON, JACQUELINE GOODRIDGE, and VIRGINIA KALDMO, Individually, on behalf of the general public, and on behalf of all others similarly situated,

Plaintiffs,

v.

EXPERIAN DATA CORP., a Delaware corporation,

Defendant.

Case No.

CLASS ACTION

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Plaintiffs Maudie Patton, Jacqueline Goodridge, and Virginia Kaldmo (collectively, "Plaintiffs"), individually and on behalf of the general public and all others similarly situated (the "Class Members"), by and through their attorneys, upon personal knowledge as to facts pertaining to them and on information and belief as to all other matters, complain of the actions of Defendant Experian Data Corp. ("Experian"), and respectfully state the following:

NATURE OF THE CASE

1. Experian sold Plaintiffs' and Class Members' highly sensitive, confidential, and regulated consumer, financial, and personal records and information, including consumer credit information and social security numbers (collectively, "PII") to an identity thief who also sold PII to other identity theft criminals. This action seeks to hold Defendant accountable for this conduct, to ensure Experian never engages in this type of conduct again, to provide notification to all Class Members and to provide redress to Plaintiffs and the other members of the Class.

2. Defendant sold and granted access to the PII of millions of U.S. citizens (*i.e.*, the "Class Members"), including Plaintiffs, to Hieu Minh Ngo ("Ngo"), a known and now convicted identity thief, black market PII trafficker, and computer hacker. In turn, Ngo sold and permitted access to PII to his customers, who themselves are identity thieves, in a scheme that lasted for several years (the "Security Lapse"). The Security Lapse is one of the largest data security lapses involving wrongfully disclosed and compromised PII in the history of the United States.

3. Ngo sold Plaintiffs' and other Class Members' PII to Lance Ealy ("Ealy"), one of Ngo's fraudster customers, and possibly other fraudster customers, the identities of whom are known only by Defendant. Ealy used all, or a part of, Plaintiffs' and Class Members' PII to file fraudulent federal income

tax returns in their names and commit other forms of identity theft and identity fraud.[1] At the time he was arrested, Ngo had 1,300 other fraudster customers who purchased and accessed Plaintiffs' and Class Members' PII for the purpose of committing fraud against the members of the Class.

4. Plaintiffs sue for Defendant's violations of the Fair Credit Reporting Act, 15 U.S.C. § 1681, *et seq.* ("FCRA"), California Business & Professions Code §§ 17200, *et seq.*, and the Declaratory Judgment Act, 28 U.S.C. § 2201, *et seq.*

5. Plaintiffs seek to recover FCRA statutory damages. Plaintiffs also seek injunctive relief requiring Defendant to, *inter alia*, (i) notify each U.S. citizen whose PII (a) was accessed by Ngo, (b) sold by Defendant to Ngo and/or his fraudster customers, or (c) was otherwise exposed in the Security Lapse, (ii) provide quality credit monitoring and substantial identity theft coverage to each such person, (iii) establish a fund (in an amount to be determined) to which such persons may apply for reimbursement of the time and out-of-pocket expenses they incurred to remediate identity theft and identity fraud (*i.e.*, data breach insurance), from July 1, 2010 forward to the date the above-referenced credit monitoring terminates, (iv) disgorge its gross revenue from transactions with Ngo and his fraudster customers involving Plaintiffs' and Class Members' PII and the earnings on such gross revenue, and (v) discontinue its above-described wrongful actions, inaction, omissions, want of ordinary care, nondisclosures, and the causes of the Security Lapse.

6. Providing Security Lapse notice will cause Defendant to comply with California's data breach notification statute, as well as the notification

[1] According to the United States Government Accounting Office (GAO), the terms "identity theft" or "identity fraud" are broad terms encompassing various types of criminal activities. Identity theft occurs when PII is used to commit fraud or other crimes. These crimes include, *inter alia*, credit card fraud, phone or utilities fraud, bank fraud and government fraud (filing fraudulent tax returns and theft of government services).

statutes of various other states. The Security Lapse notice, as well as the above-referenced protections, also will fulfill the promise made to Congress by Tony Hadley, Experian's Senior Vice President of Government Affairs and Public Policy, that "we know who they [the Security Lapse victims] are, and we're going to make sure they're protected."

7. Notice will provide Security Lapse victims (*i.e.*, Plaintiffs and Class Members) with an explanation of the Security Lapse, so they will be vigilant and take the appropriate remedial and protective measures. Providing notice also is not only the right thing to do but the legally mandated thing to do. Without individualized notice, Security Lapse victims do not know whether or how their PII was compromised, the categories of PII compromised, and the types of identity theft and identity fraud to which they have been exposed or actually suffered. The Security Lapse notice also will alleviate concerns and bring peace of mind to individuals whose PII was not sold or made available to Ngo and his fraudster customers by Defendant. Security Lapse notice is the logical first step in restoring the security of Plaintiffs' and Class Members' PII wrongfully disclosed in the Security Lapse.

8. As professed experts in data breach management, Defendant knows well that the law requires that victims of a data breach, such as the Security Lapse, be notified about the unauthorized disclosure of their PII. As an avid purveyor of credit monitoring and other data breach remediation products, reaping huge revenues from their representations, Defendant also knows the undisputable benefits that credit monitoring, expense reimbursement funds (*i.e.*, data breach insurance), and other data breach remediation products provide.

9. Plaintiffs have standing to bring this suit under FCRA because Defendant wrongfully and willfully disclosed their PII without authorization for no permissible purpose. Plaintiffs also have standing to bring this suit because as a direct and proximate result of Defendant's wrongful actions, inaction,

omissions, willful disregard and conduct, and want of ordinary care, and the resulting Security Lapse, they have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*, (i) actual identity theft and identity fraud, (ii) invasion of privacy, (iii) loss of the intrinsic value of their privacy, (iv) breach of the confidentiality of their consumer reports and PII, (v) deprivation of the value of their PII, for which there is a well-established national and international market,[2] (vi) the financial and temporal cost of monitoring their credit, monitoring their financial accounts, and mitigating their damages, and (vii) the imminent, immediate, and continuing increased risk of ongoing identity theft and identity fraud. Plaintiffs also have standing to bring this suit because Defendant has yet to send the required Security Lapse notice.

10. Plaintiffs and Class Members need identity theft and credit protection as a result of Defendant's sale of PII to known thieves, just as the cost of such protections are a reasonably necessary expense for the protection of the federal employees victimized by the massive data breach at the U.S. Office of Personnel Management ("OPM") in June 2015.[3] In addition, Plaintiffs are entitled to other money damages, statutory and under common law, therefore, on

---

[2] PII is a valuable property right. *See, e.g.*, John T. Soma, *et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 RICH. J.L. & TECH. 11, at *3-*4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted). It is so valuable to identity thieves that once PII has been compromised, criminals often trade it on the "cyber black-market" for several years.

[3] *See* Bob McGovern, Judges Under Fire, Boston Herald, July 11, 2015 at http://www.bostonherald.com/news_opinion/local_coverage/2015/07/judges_under_fire (last visited July 14, 2015) (reporting that although federal judges victimized by the recent OPM data breach will "automatically receive $1 million of identity theft insurance and access to full-service identity restoration services," they are dissatisfied with the fact that the offered "credit monitoring services are available for only 18 months and none of the services cover family members." According to Administrative Office Director James Duff, "[b]oth the scope and duration of the services concern us, as well as many of our judges and employees. We are voicing our concerns about these issues.").

behalf of themselves and Class Members, additionally seek (i) statutory FCRA damages, (ii) declaratory relief, (iii) injunctive relief, and (iv) attorneys' fees, litigation expenses, and court costs.

JURISDICTION AND VENUE

11. This Court has subject matter jurisdiction over Plaintiffs' FCRA claims pursuant to 28 U.S.C. § 1331 (federal question). This Court also has subject matter jurisdiction over Plaintiffs' claims under 28 U.S.C. § 1332(d) (CAFA) because (i) this action is brought as a class action under FED. R. CIV. P. 23, (ii) there are 100 or more Class Members, (iii) at least one Class member is a citizen of a state diverse from Defendant's citizenship, and (iv) the matter in controversy exceeds $5,000,000 exclusive of interest and costs. This Court also has jurisdiction over Plaintiffs' state law claims pursuant to 28 U.S.C. § 1367. This Court has personal jurisdiction over Defendant because at all relevant times, its headquarters and principal places of business were (and continue to be) in the Central District of California, and Defendant conducted (and continues to conduct) business in the Central District of California.

12. Venue is proper in the Southern Division of the Central District of California, Southern Division, under 28 U.S.C. § 1391(b) and (c), because a substantial part, if not all, of the events giving rise to this action occurred in this Division, and Experian's operational headquarters in the United States is in Costa Mesa, California and it conducts business in this Division of this District.

PARTIES

13. Plaintiff Maudie Patton is a citizen and resident of Roswell, New Mexico. Patton's PII was purchased and accessed by Ngo from Experian, CVI, and U.S. Info Search databases, either directly or indirectly through Ngo's black market websites, Superget.info and findget.me. At least one of Ngo's fraudster customers (Ealy), and possibly others, used her PII without authorization to file a fraudulent federal income tax return in her name and commit other acts of

identity theft and/or identity fraud. Patton is concerned about her PII, finances, credit, and identity and, as such, regularly monitors her credit and financial accounts, and carefully stores and disposes of PII and other documents containing PII.

14. Plaintiff Jacqueline Goodridge is a citizen and resident of Coos Bay, Oregon. Goodridge's PII was purchased and accessed by Ngo from Experian, CVI, and U.S. Info Search databases, either directly or indirectly through Ngo's black market websites, Superget.info and findget.me. At least one of Ngo's fraudster customers (Ealy), and possibly others, used her PII without authorization to file a fraudulent federal income tax return in her name and commit other acts of identity theft and/or identity fraud. Goodridge is concerned about her PII, finances, credit, and identity and, as such, regularly monitors her credit and financial accounts, and carefully stores and disposes of PII and other documents containing PII.

15. Plaintiff Virginia Kaldmo is a citizen and resident of Amelia, Ohio. Kaldmo's PII was purchased and accessed by Ngo from Experian, CVI, and U.S. Info Search databases, either directly or indirectly through Ngo's black market websites, Superget.info and findget.me. At least one of Ngo's fraudster customers (Ealy), and possibly others, used her PII without authorization, in whole or in part, to file a fraudulent federal income tax return in her name and commit other acts of identity theft and/or identity fraud. Kaldmo is concerned about her PII, finances, credit, and identity and, as such, regularly monitors her credit and financial accounts, and carefully stores and disposes of PII and other documents containing PII.

16. Defendant Experian Data Corp. is a Delaware corporation with its principal place of business in Costa Mesa, California. Experian is a wholly-owned subsidiary of the Republic of Ireland company, Experian plc, and a "consumer reporting agency" as defined in 15 U.S.C. § 1681a(f), in that at all

relevant times, Experian regularly engaged (and continues to regularly engage) in the business of assembling, evaluating, and dispersing information concerning consumers for the purpose of furnishing consumer reports, as defined in FCRA, to third parties. In March 2012, Experian acquired certain assets and liabilities owned by Court Ventures, Inc. ("CVI"), including the CVI Database. As a result, Experian became the successor in interest to CVI's assets, business, and related liabilities. Experian may be served with Summons and a copy of this Class Action Complaint by serving its registered agent for service of process, C.T. Corporation System, 818 West Seventh Street, Second Floor, Los Angeles, California 90017.

17. Experian is part of a global information services group of companies, providing data and analytical tools to its clients around the world. According to its parent's website, https://www.experianplc.com (last visited on July 17, 2015), the Experian companies "help businesses to manage credit risk, prevent fraud, target marketing offers and automate decision making" and "help people to check their credit report and credit score, and protect against identity theft."

18. Experian collects information on people, businesses, motor vehicles, insurance, and lifestyle data, including data pertaining to United States citizens and residents. Experian's principal lines of business are credit services, marketing services, decision analytics, and consumer services—with, among other things, a claimed expertise in fraud detection.[4]

[4] *See* http://www.experian.com/corporate/areas-of-expertise.html (last visited April 14, 2015) and http://www.experian.com/corporate/fraud-detection.html (last visited April 14, 2015) (recognizing, among other things, that "[f]raud is a huge issue that is on the rise," "[t]here is a constant, ongoing battle between fraudsters and legitimate businesses, particularly in the area of digital security," "[t]here is a high social and financial cost to fraud that impacts both organizations and individuals," and "[h]undreds of fraudulent techniques exist, which include anything from theft of a credit or debit card, tax evasion, claims fraud, advertising goods and services that don't exist, falsifying information, or stealing another's identity for gain.").

BACKGROUND

I. The Ngo Identity Fraud Operation and the Security Lapse

19. In or around late 2010, Ngo, a Vietnamese hacker, fraudulently posed as a private investigator from Singapore named "Jason Low" "doing business" as "SG Investigators," and contracted with CVI for access to its U.S. consumer PII databases. According to the ruse, SG Investigators was employed by a large company to conduct background checks on job applicants.

20. At all relevant times CVI was in the business of aggregating public record court data, such as criminal records, civil suits and judgments, state tax liens, marriage licenses, death certificates, professional business licenses, and bankruptcy petitions, discharges, and dismissals. CVI aggregated this data from more than 1,400 state and county record repositories. Its databases, which are owned by Experian, collect data from sources representing more than 80% of the U.S. population.

21. Ngo's relationship with CVI gave him access to more than just CVI's databases. At all relevant times, CVI had a reciprocity agreement with Ohio-based data broker U.S. Info Search, whereby the two entities' shared information from, and access to, each other's databases. As such, CVI and U.S. Info Search subscribers had complete access to both companies' U.S. consumer PII databases.

22. Because CVI and U.S. Info Search openly granted access to each other's subscribers, Ngo accessed the PII of more than 200 million Americans including, *inter alia*, criminal and civil judgment histories, bankruptcy histories, tax lien histories, professional business licenses, marital status, Social Security

---

Experian also boasts that "[f]raud detection and identity management products or services permeate throughout Experian, enabling companies to detect, monitor and assess the risk of fraud at every stage of their customer relationship" and touts its ability to detect cases of fraud, automate fraud risk assessment, predict the likelihood of fraud, reduce may types of fraud, and establish shared fraud detection schemes across multiple organizations in a particular industry. *Id.*

numbers, addresses, dates of births, personal vital statistics, and bank information.

23. Ngo, posing as SG Investigators, was one of CVI's biggest clients. Ngo regularly wired CVI $15,000 per month from his bank account in Singapore for access to CVI's and U.S. Info Search's consumer PII databases through his CVI account.

24. During July 2010, Ngo commenced reselling U.S. consumer PII from, and granting access to, the CVI and U.S. Info Search consumer PII databases through the known fraudster websites, Superget.info and findget.me, which Ngo created and operated. The Superget.info and findget.me websites were hosted by servers located overseas. Registration was free and anonymous. The websites accepted payment in the form of virtual currency, including Liberty Reserve, which the federal government alleges is responsible for laundering over $6 billion of proceeds from criminal activity.

25. The Superget.info and findget.me websites were user friendly, "interfacing" directly with CVI's databases and serving as consumer PII superhighways. The websites were direct consumer PII conduits from CVI's databases (and U.S. Info Search's databases) to Ngo's illicit clientele.

26. Superget.info, for example, operated in such a way that a visitor could enter a name and a state of residence of a prospective victim, and obtain other PII relating to the victim from CVI's databases and U.S. Info Search's databases, including the victim's complete name, age, date of birth, address, and Social Security number. A successful hit on a Social Security number or date of birth cost a fraudster approximately $3.00, which Ngo collected. At one time, Superget.info boasted that "[a]bout 99% nearly 100% US people could be found, more than any sites on the internet now."

27. Ngo's websites also sold "fullz," which is fraudster slang for a complete collection of a prospective identity theft victim's PII. Fullz are used to

open new financial accounts, including credit card accounts, make purchases, transfer funds from accounts, obtain loans in the victim's name, and file fraudulent income tax returns in the victim's name and intercept the refunds. A fullz, which typically sells for about $8.00 on the black market, includes a person's full name, maiden name, work history, e-mail accounts, various account passwords, medical history, address, telephone number, driver's license numbers, Social Security number, birthdate, checking/savings account numbers, and routing numbers.

28. It has so far been established that the Superget.info and findget.me websites had 1,300 customers who paid Ngo nearly $2 million over the relevant period to access databases containing the PII of 200 million U.S. citizens. Over an 18-month period, Superget.info customers conducted approximately 3.1 million queries, 1.0 million of which were conducted *after* Experian acquired CVI. Since each query could generate an unlimited number of hits, the actual number of individual consumer PII records exposed, accessed, obtained, and utilized by fraudsters to commit further identity theft and identity fraud could be in the tens of millions.

29. In February 2013, the U.S. Secret Service arrested Ngo. On July 14, 2015, Ngo was sentenced to 13 years in prison for hacking into U.S. businesses' computers, stealing PII, and selling to his cybercriminal customers the fraudulently-obtained access to PII in the Experian, CVI, and U.S. Info Search databases belonging to approximately 200 million U.S. citizens.[5]

II. Experian's and CVI's Involvement in the Security Lapse

30. In March 2012, Experian bought CVI, including the rights and obligations under CVI's data reciprocity agreement with U.S. Info Search, for

[5] *See* Press Release, U.S. Department of Justice, Vietnamese National Sentenced to 13 Years in Prison for Operating a Massive International Hacking and Identity Theft Scheme (July 14, 2015) at http://www.justice.gov/opa/pr/vietnamese-national-sentenced-13-years-prison-operating-massive-international-hacking-and (last visited July 15, 2015).

about $18.3 million.

31. When conducting due diligence prior to the acquisition of CVI, Experian learned several facts that should have alerted it that CVI engaged in, and was connected to, unauthorized and unlawful activity, including Ngo's identity fraud operation. For example, CVI represented to Experian that virtually all of the data it sold was publicly available criminal history information, and thus unregulated. But, Experian later learned prior to the purchase that CVI, in fact, accessed certain personal information and, therefore, was subject to regulation. Prior to acquiring CVI, Experian learned that CVI misrepresented its regulatory compliance regarding such information.

32. When conducting due diligence prior to the acquisition of CVI, Experian also discovered the fact that the largest buyer of consumer PII was SG Investigators, a Singapore-based private investigator who made substantial monthly wire transfers from its bank in Singapore in payment for accessing CVI's consumer PII databases.

33. Based on this information, Experian should have further investigated CVI's regulatory compliance, Ngo, and SG Investigators' operations. Had Experian performed even the most basic additional investigation of Ngo and SG Investigators, Experian would have discovered Ngo's illegal identity fraud enterprise utilizing CVI's consumer PII databases, and shut it down. Experian, however, intentionally or with reckless disregard failed to do so, stood willingly by, facilitated the illicit operation, and reaped the financial benefits of the acquisition of CVI for another ten months.

34. Shortly after acquiring CVI, Experian learned that CVI was unlawfully obtaining public record information through a practice known as "web scraping." Web scraping is prohibited by many of CVI's public record information sources, but CVI web scraped these sites anyway, in violation of the sites' terms of use. In doing so, CVI created workarounds that sidestepped such

websites' technological barriers that were designed to prevent web scraping. Thus, both before and immediately after Experian acquired CVI, it was acutely aware of serious issues with CVI's operations that should have caused Experian to launch a thorough and comprehensive internal investigation of CVI to right the ship.

35. For almost ten months after Experian acquired CVI, Ngo paid Experian a substantial amount of money for continued access to a now-expanded treasure trove of consumer PII databases owned and operated by Experian, CVI, and U.S. Info Search. Experian accepted Ngo's payments "with no questions asked." Approximately 1.0 million database queries were made by Ngo and his fraudster customers during this time, for which, according to Marc Martin, the CEO of U.S. Info Search, Experian collected up to $500,000 or more.

36. It was only when the U.S. Secret Service notified Experian in November 2012 about its ongoing investigation of Ngo that Experian began to take action—even though before this date, Experian was in possession of several facts sufficient to put it on inquiry notice of the Security Lapse. For example, by that time, Experian had the logs of Ngo's activity and could have learned that Ngo (for his customers) was inputting millions of names and states of residence in order to obtain Social Security numbers, dates of birth, financial accounts information, and other PII. Experian failed to investigate Ngo further until federal authorities contacted Experian and notified it about their investigation. Even without notice, however, Experian should have monitored its transactions in the normal course of its consumer credit reporting and data brokering business. Its failure to do so resulted in the continuation and expansion of the Security Lapse.

37. Ever since federal authorities forced Experian's hand, Experian has been trying to pass the buck. In a contract dispute pending in California state court, Experian concedes that CVI sold consumer data to Ngo "without having

vetted to see if he qualified to obtain such information and Ngo in turn sold this information to many hundreds of identity thieves situated all over the world." Experian admits that as successor in interest to CVI's business, assets, and liabilities, CVI's actions exposed Experian to liability to potential liability, governmental scrutiny, fines, penalties, loss of revenues, and damages.[6] An Experian executive also testified before Congress, admitting that during Experian's "due diligence" of CVI Experian did not obtain "all of the information necessary to vet" CVI's business activities, including its relationship with Ngo. Defendant's attempted cover up is only surpassed by its initial conduct: the Security Lapse itself.

III. Security Lapses Lead to Identity Theft and Identity Fraud

38. Identity theft occurs when a person's PII, such as his or her name, e-mail address, address, Social Security number, billing and shipping addresses, telephone number, and payment card information is used without authorization to commit fraud or other crimes.

39. According to the Federal Trade Commission ("FTC"), "the range of privacy-related harms is more expansive than economic or physical harm or unwarranted intrusions" and "any privacy framework should recognize additional harms that might arise from unanticipated uses of data."[7] There "is significant evidence demonstrating that technological advances and the ability to combine disparate pieces of data can lead to identification of a consumer, computer or device even if the individual pieces of data do not constitute [PII]."[8]

[6] Cross-Complaint ¶6, *Court Ventures, Inc. v. Experian Data Corp.*, No. 30-2013-00682410-CU-BC-CJC (Cal. Super. Ct. Feb. 28, 2014).

[7] FTC Report, *Protecting Consumer Privacy in an Era of Rapid Change*, 8 (March 2012), available at http://www.ftc.gov/os/2012/03/120326privacyreport.pdf (last visited May 8, 2014).

[8] *Id.*: *Comment of Center for Democracy & Technology*, cmt. #00469, at 3; *Comment of Statz, Inc.*, cmt. #00377, at 11–12.

40. In fact, while reflecting on the recent OPM data breach, David Sellers, a spokesman for the Administrative Office of the U.S. Courts, opined that "[i]t is certainly a matter of grave concern, as is the case with any security issue.... [I]t is not that different than some kind of a disaster. It is of that proportion. The potential for disaster is humongous."[9]

41. Providing meaningful identity theft monitoring and identity theft insurance are widely recognized as necessary for every person whose PII is taken. For example, the federal government is providing identity theft monitoring, identity theft insurance and restoration services to all 21.5 million victims affected by the OPM data breach.[10] The federal government believes these measures (as well as others) are necessary regardless of who was affected by the data breach.

42. Because Plaintiffs' and Class Members' Social Security numbers were disclosed without authorization for an improper purpose, they face an imminent, immediate and continuing increased risk of identity theft and identity fraud—similar to that of the federal judiciary as a result of the recent OPM data breach.

43. Javelin Strategy & Research ("Javelin"), a leading provider of quantitative and qualitative research, releases Identity Fraud Reports quantifying the impact of data security breaches. According to Javelin's 2012 report, individuals whose PII is subject to a reported security breach—such as the Security Lapse at issue here—are approximately 9.5 times more likely than the general public to suffer identity fraud and/or identity theft. Javelin's most recent report shows that the total amount stolen in 2013 reached $18 billion. In 2013, one in three people who received data breach notification letters became a victim

[9] *See* Bob McGovern, *Judges Under Fire*, BOSTON HERALD, July 11, 2015 at http://www.bostonherald.com/news_opinion/local_coverage/2015/07/judges_under_fire (last visited July 14, 2015).

[10] *See* Information about OPM Cybersecurity Incidents, https//www.opm.gov/cybersecurity, last visited July 16, 2015.

of fraud, 46% of consumers with breached debit cards became a victim, and 16% of consumers with a breached Social Security number experience fraud.

44. According to the FTC, victims of identity theft and identity fraud are at serious risk of substantial losses. "Once identity thieves have your personal information, they can drain your bank account, run up charges on your credit cards, open new utility accounts, or get medical treatment on your health insurance. An identity thief can file a tax refund in your name and get your refund. In some extreme cases, a thief might even give your name to the police during an arrest."[11]

45. Identity thieves use Social Security numbers to commit other types of fraud. The Government Accounting Office (GAO) found that identity thieves use PII to open financial accounts and payment card accounts and incur charges in a victim's name.[12] This type of identity theft can be the most damaging because it may take some time for the victim to become aware of the theft, while in the meantime causing significant harm to the victim's credit rating and finances. Moreover, unlike other PII, Social Security numbers are incredibly difficult to change, and their misuse can continue for years into the future.

46. Identity thieves also use Social Security numbers to obtain false identification cards, obtain government benefits in the victim's name, commit crimes, and, as occurred here, file fraudulent tax returns to pilfer the victims' tax refunds. Identity thieves also obtain jobs using stolen Social Security numbers, rent houses and apartments, and obtain medical services in the victim's name. Identity thieves also have been known to give a victim's personal information to police during an arrest, resulting in the issuance of an arrest warrant in the victim's name and an unwarranted criminal record. The GAO states that victims

[11] *See* FTC, *Signs of Identity Theft*, available at http://www.consumer.ftc.gov/articles/0271-signs-identity-theft (last visited July 17, 2015).

[12] *See* Government Accountability Office. *Personal Information*. 9 (June 2007), *available at* http://www.gao.gov/new.items/d07737.pdf (last visited July 17, 2015).

of identity theft face "substantial costs and inconvenience repairing damage to their credit records," as well the damage to their "good name."[13]

47. The unauthorized disclosure of a person's Social Security number can be particularly damaging, because Social Security numbers cannot be easily replaced like a credit card or debit card. In order to obtain a new Social Security number, a person must show evidence that someone is using the number fraudulently, as well as show that he has done all he can to fix the problems resulting from the misuse.[14] Thus, individuals whose PII has been stolen cannot obtain a new Social Security number until the damage has already been done and they have shown they have done all they can to fix the problems.

48. Obtaining a new Social Security number does not absolutely prevent continued identity fraud. Government agencies, private businesses, and credit reporting companies likely still have the person's records under the old number, so the effects of the identity theft may persist long after the incident. For some victims of identity theft, a new number may actually create more problems. Because prior positive credit information is not associated with the new Social Security number, it is more difficult to obtain credit due to the absence of a credit history.

49. PII is a valuable commodity to identity thieves. Once PII has been compromised, criminals often trade the information on the "cyber black market" for a number of years.[15] Identity thieves and other cyber criminals openly post stolen credit card numbers, Social Security numbers, and other personal financial

---

[13] *See* Government Accountability Office. Identity Theft. 2 (PDF pagination) (June 17, 2009) http://www.gao.gov/new.items/d09759t.pdf (last visited July 17, 2015).

[14] *See* Identity Theft and Your Social Security Number, SSA Publication No. 05-10064, October 2007, ICN 46327, available at http://www.ssa.gov/pubs/10064.html (last visited July 17, 2015).

[15] Companies, in fact, also recognize PII as an extremely valuable commodity akin to a form of personal property. *See* T. Soma, *et al*, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 Rich. J.L. & Tech. 11, 3–4 (2009).

information on various Internet websites, thereby making the information publicly available. In one study, researchers found hundreds of websites displaying stolen personal financial information. Strikingly, none of these websites was blocked by Google's safeguard filtering mechanism—the "Safe Browsing list." One study concluded:

> It is clear from the current state of the credit card black-market that cyber criminals can operate much too easily on the Internet. They are not afraid to put out their email addresses, in some cases phone numbers and other credentials in their advertisements. It seems that the black market for cyber criminals is not underground at all. In fact, it's very "in your face."[16]

IV. Ngo and His Customers Have Been Convicted of Identity Fraud Crimes for Utilizing Plaintiffs' and Class Members' PII Without Authorization

50. After Ngo was apprehended, federal authorities identified and located some of Ngo's fraudster customers. In interviews with federal authorities, Ngo's customers admitted that they intended to use, and used, the PII obtained from the Experian, CVI, and U.S. Info Search databases through Ngo's websites to engage in criminal fraud.

51. For example, on November 18, 2014, Lance Ealy was convicted of 46 counts of wire fraud and identity theft for fraudulently obtaining consumer PII from Experian, CVI, and U.S. Info Search databases through Ngo's websites, using the PII, in whole or in part, to electronically file fraudulent federal income tax returns—including tax returns in Plaintiffs' names and the names of over 175 other persons—and intercepting the tax refund checks worth thousands of dollars.[17]

---

[16] StopTheHacker, *The "Underground" Credit Card Blackmarket*, *available at* http://www.stopthehacker.com/2010/03/03/the-underground-credit-card-black market/ (last visited July 17, 2015).

[17] The government currently estimates that 13,673 fraudulent federal income tax returns reflecting over $64.7 million of fraudulent tax refunds were filed by Ngo's fraudster customers using Plaintiffs' and Class Members' PII purchased from Defendant. *See* http://www.justice.gov/opa/pr/vietnamese-national-

52. During the trial, the federal government offered evidence that Ngo sent PII for each of the Plaintiffs to Ealy via email sometime in late January 2013—almost three months after the U.S. Secret Service notified Experian of the Security Lapse.

53. On March 31, 2014, another Ngo fraudster customer, Idris Soyemi, pleaded guilty to one count of wire fraud arising out of dealings with Ngo. According to the federal prosecutor at the plea hearing:

> [E]-mail communications between Mr. Soyemi and Mr. Ngo would establish that Mr. Soyemi was purchasing on numerous occasions PII from Mr. Ngo . . . of dozens, if not hundreds, of individuals in the United States for the purpose of engaging in criminal conduct, including credit card fraud and bank fraud, so that Mr. Soyemi could then falsely represent that he was the actual person in whose name he was applying for credit card accounts to obtain merchandise through that false representation and also to obtain money from banks through the false representation that he was the person associated with that bank account.[18]

54. On information and belief, the PII Soyemi sought to obtain, obtained, and used to fraudulently obtain credit card accounts and file fraudulent tax returns was obtained, in whole or in part, from the Experian, CVI, and U.S. Info Search databases through Ngo's websites.

55. Numerous other individuals have been implicated, indicted, convicted, or pleaded guilty to identity theft/identity fraud schemes connected to Plaintiffs' and Class Members' PII obtained, in whole or in part, from the Experian, CVI, and/or U.S. Info Search databases through Ngo's websites—including Oluwaseun Adekoya (D.N.H.), Joe Daniels (D. Mass.), Derric Theoc (D.N.H.), and Quentin Hall, aka "Swipe Life" (D.N.H.).

///

///

---

sentenced-13-years-prison-operating-massive-international-hacking-and (last visited July 15, 2015).

[18] *United States v. Soyemi*, 13-cr-96-01-PB, Tr. of Change of Plea Hearing at 14 (D.N.H. Mar. 31, 2014).

V. Experian Refuses to Notify the Victims of Ngo's Identity Fraud Operation or Provide Them with Protection Even Though Experian Knows Their Identities, and Its Senior Vice President Promised Congress Experian Would "make sure they're protected"

56. According to its website, Experian "considers itself a steward of the information it collects, maintains and utilizes. [Its] responsibility is to ensure the security of the information in [its] care and to maintain the privacy of consumers through appropriate, responsible use."[19]

57. Experian further promises on its website that "[w]e use a variety of security systems to safeguard the information we maintain and provide"; and "[w]e maintain physical security for our facilities and limit access to critical areas; and we conduct approval processes before information Experian maintains can be accessed or changed."[20]

58. The Security Lapse has revealed these assurances to be untrue. And, even though Experian considers itself a steward of consumer reports, Experian has not notified the consumers affected by the Security Lapse, or provided them with protection—such as credit monitoring—despite the ethical, moral, and legal requirement to do so.

59. After being alerted to the Ngo identity fraud operation, Experian continued its tangled web of contradictions. In a March 30, 2014 Experian press release, Gerry Tschopp, Experian's Senior Vice President of Public Affairs and Public Relations, stated that "[i]n terms of notifying consumers, Experian does not know which consumers' information was disclosed as the data did not come from an Experian database and no other information now available to Experian would identify which consumers should be notified." Experian's resources, technological capabilities, line of business (including data breach management

[19] "Our Approach to Privacy", https://www.experian.com/privacy/ (last visited July 16, 2015).

[20] "Upholding Our Information Values", http://www.experian.com/privacy/information_values.html (last visited July 16, 2015).

and business consulting), and statements by another senior executive suggests that Tschopp's statement is not true.

60. For example, at a December 18, 2013 hearing of the Senate Committee on Commerce, Science, and Transportation addressing possible legislation concerning the use of consumer information for marketing purposes, Tony Hadley, Experian's Senior Vice President of Government Affairs and Public Policy, testified, under oath, about the Ngo identity fraud victims, stating "we know who they are, and we're going to make sure they're protected."[21] Senator McCaskill expressed concern that the Security Lapse demonstrated that Experian is not a capable steward of the consumer information it collected and shared for marketing purposes. More importantly, and setting aside the fact that Hadley's statement directly contradicts Tschopp's statement, Experian has not made good on Hadley's promise.

61. Consistent with Hadley's statement, Experian's allegations in its cross-complaint against Court Ventures in the California state court litigation indicate that the PII sold by Experian and CVI to Ngo and his fraudster customers is readily ascertainable by Experian. Experian specifically alleges:

> It was only as a result of [the U.S. Secret Service contacting Experian] that Experian had any reason to look at the actual logs for SG Investigators' queries, at which point Experian discovered that SG Investigators was inputting names and states in order to obtain consumers' social security numbers.[22]

The fact that Experian is able to ascertain the identity of the victims of the Ngo identity fraud operation from its logs through reasonable efforts, coupled with the record evidence in the criminal trials of Ngo, Ealy, Soyemi, and other Ngo fraudster customers, confirm that any pretext for Experian's failure and refusal to

---

[21] Congressional Hearing Commerce, Science, and Transportation Committee, available at http://www.commerce.senate.gov/public/index.cfm?p=Hearings&ContentRecord_id=a5c3a62c-68a6-4735-9d18-916bdbbadf01&ContentType_id=14f995b9-dfa5-407a-9d35-56cc7152a7ed&Group_id=b06c39af-e033-4cba-9221-de668ca1978a at 2:22:30.

[22] Cross-Complaint ¶18, *Court Ventures, Inc. v. Experian Data Corp.*, No. 30-2013-00682410-CU-BC-CJC (Cal. Super. Ct. Feb. 28, 2014).

provide notice to, and credit monitoring for, the victims is false.

62. Experian's failure and refusal to do so is particularly egregious in light of Experian's self-touted expertise in data breach management. Indeed, Experian's Data Breach Response Guide emphasizes the importance of implementing an effective notification program.[23] Experian's failure to take its own advice to rectify a serious situation that it created, is willful, reckless, and designed to forestall the investigation and obstruct justice. Physician, heal thyself.[24]

63. Defendant's failure and refusal to safeguard and protect Plaintiffs' and Class Members' PII, and Experian's failure and refusal to, *inter alia*, (i) properly conduct its due diligence of CVI before acquiring it, (ii) thoroughly and completely investigate the Ngo identity fraud operation after obtaining full knowledge about Ngo and the substantial amount of money he sent CVI and Experian every month, (iii) notify Plaintiffs and Class Members about the Security Lapse, and (iv) provide them with protection after promising Congress that it would do so has caused (and will continue to cause) Plaintiffs and Class Members to suffer the above-described economic damages, and other injury and harm.

CLASS ACTION ALLEGATIONS

64. Pursuant to Rule 23 of the Federal Rules of Civil Procedure, Plaintiff brings this action as a class action individually, and on behalf of the following Class of similarly situated individuals:

> All persons whose personally identifiable information (PII) (i) was accessed by Hieu Minh Ngo or his customers, (ii) sold by Defendant to Hieu Minh Ngo or his customers, or (iii) otherwise exposed in the Security Lapse, whether directly or indirectly through Hieu Minh

[23] *See* Data Breach Response Guide 13 (2014), available at http://www.experian.com/assets/data-breach/brochures/2014-2015-data-breach-response-guide.pdf (last visited July 16, 2015).

[24] LUKE 4:23 (KJV).

Ngo's websites, Superget.info and findget.me, from July 1, 2010 to the present.

Excluded from the Class are (i) Defendant and its owners, officers, directors, employees, agents, representatives, parent companies, subsidiaries, affiliates, successors, and assigns; and (ii) the Court, Court personnel, and members of their immediate families.

65. The Class Members are so numerous that their joinder would be impracticable. Class members potentially number in the millions. The precise number of Class Members is presently unknown to Plaintiffs, but may be ascertained from Defendant's records. Disposition of this matter as a class action will provide substantial benefits and efficiencies to the Parties and the Court.

66. Common questions of law and fact exist as to all Class Members, and predominate over any individual questions including, *inter alia*:

(i) whether Defendant failed to safeguard and protect Plaintiffs' and Class Members' PII;

(ii) whether Experian failed to properly conduct its due diligence prior to acquiring CVI;

(iii) whether Experian failed to properly investigate Ngo and his operations after learning about him;

(iv) whether Defendant failed to notify Plaintiffs and Class Members whose PII was accessed and/or obtained without authorization in the Security Lapse;

(v) whether Defendant violated applicable data breach notification laws by failing to notify Plaintiffs and Class Members whose PII was accessed and/or obtained without authorization in the Security Lapse;

(vi) whether Experian failed to protect Plaintiffs and Class Members as promised to Congress;

(vii) whether Defendant's failure to notify Plaintiffs and Class Members whose PII was accessed and/or obtained without authorization in the

Security Lapse was an unlawful, unfair, and/or fraudulent business practice in violation of the California Business & Professions Code § 17200;

(viii) whether Defendant's failure to notify caused or aggravated Plaintiffs and Class members economic injury in fact; and

(ix) whether and to what extent Plaintiffs and Class Members are entitled to declaratory and injunctive relief.

Defendant engaged in uniform wrongful actions, inaction and omissions giving rise to the legal rights sought to be enforced by Plaintiffs, individually and on behalf of Class Members.

67. Plaintiffs' claims are typical of Class Members' claims in that Plaintiffs' claims and Class Members' claims all arise from Defendant's uniform wrongful actions, inaction and omissions, and willful misconduct; to wit, Defendant's failure and refusal to safeguard and protect Plaintiffs' and Class Members' PII, and Experian's failure and refusal to, *inter alia*, (i) properly conduct its due diligence of CVI before acquiring it, (ii) thoroughly and completely investigate the Ngo identity fraud operation after obtaining full knowledge about Ngo and the substantial amount of money he sent CVI and Experian every month, (iii) notify Plaintiffs and Class Members about the Security Lapse, and (iv) provide Plaintiffs and Class Members with protection after promising Congress that it would do so.

68. Plaintiffs and their counsel will fairly and adequately represent Class Members' interests. Plaintiffs have no interests antagonistic to, or in conflict with, Class Members' interests. Plaintiffs' attorneys are highly experienced in prosecuting consumer class actions and data security breach class actions, and will vigorously prosecute this action on behalf of Plaintiffs and Class Members.

69. Class certification, therefore, is appropriate under FED. R. CIV. P. 23(b)(3) because the above common questions of law or fact predominate over any

questions affecting individual Class Members, and a class action is superior to other available methods for the fair and efficient adjudication of this controversy.

70. Certification also is appropriate under FED. R. CIV. P. 23(b)(2) because Defendant has acted, or refused to act, on grounds generally applicable to the Class, thereby making appropriate final injunctive relief and declaratory relief with respect to the Class as a whole.

71. Certification also is appropriate under FED. R. CIV. P. 23(b)(1) because the prosecution of separate actions by individual Class Members would create a risk of establishing incompatible standards of conduct for Defendant. For example, one court might decide that the challenged actions are illegal and enjoin Defendant, while another court might decide that the same actions are not illegal. Individual actions also could be dispositive of the interests of the other Class Members who were not parties to such actions and substantially impair or impede their ability to protect their interests.

CLAIMS FOR RELIEF AND CAUSES OF ACTION

COUNT I

WILLFUL VIOLATION OF THE FAIR CREDIT REPORTING ACT

(15 U.S.C. § 1681, *et seq.*)

72. The preceding factual statements and allegations are incorporated by reference.

73. In enacting FCRA, Congress made several findings, including that consumer reporting agencies have assumed a vital role in assembling and evaluating consumer credit information and other consumer information—such as PII (15 U.S.C. § 1681(a)(3))—and "*[t]here is a need to insure* that consumer reporting agencies exercise their grave responsibilities with fairness, impartiality, and *a respect for the consumer's right to privacy*." 15 U.S.C. § 1681(a)(4) (emphasis added).

74. Under 15 U.S.C. § 1681a(f), a "consumer reporting agency" includes any person which, for monetary fees or on a cooperative nonprofit basis, regularly engages, in whole or in part, in the practice of assembling or evaluating consumer credit information or other consumer information for the purpose of furnishing "consumer reports" to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports.

75. Under 15 U.S.C. § 1681a(d)(1), a "consumer report" is any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living, which is used, expected to be used, or collected, in whole or in part, for the purpose of serving as a factor in establishing the consumer's eligibility for (i) credit or insurance to be used primarily for personal, family, or household purposes, (ii) employment purposes, or (iii) any other purpose authorized by 15 U.S.C. § 1681b.

76. "Consumer credit information" (PII) includes, *inter alia*, a person's name, identification number (*e.g.*, Social Security number), marital status, physical address and contact information, educational background, employment, professional or business history, financial accounts and financial account history (*i.e.*, details of the management of the accounts), credit report inquiries (*i.e.*, whenever consumer credit information is requested from a credit reporting agency), judgments, administration orders, defaults, and other notices.

77. FCRA limits the dissemination of "consumer credit information" (PII) to certain well-defined circumstances and no other. 15 U.S.C. § 1681b(a).

78. At all relevant times, Defendant was (and continues to be) a consumer reporting agency under FCRA because on a cooperative nonprofit basis and for monetary fees, it regularly (i) received, assembled and/or evaluated

Plaintiffs' and Class Members' "consumer credit information" protected by FCRA (*i.e.*, their PII) for the purpose of furnishing consumer reports to third parties, and (ii) used the means and facilities of interstate commerce to prepare, furnish and transmit consumer reports containing Plaintiffs' and Class Members' PII to third parties (and continues to do so).

79. As a consumer reporting agency, Defendant was (and continues to be) required to identify, implement, maintain and monitor the proper data security measures, policies, procedures, protocols, and software and hardware systems to safeguard, protect and limit the dissemination of consumer credit information in its possession, custody and control, including Plaintiffs' and Class Members' PII, only for permissible purposes under FCRA. *See* 15 U.S.C. § 1681(b).

80. By its above-described wrongful actions, inaction and omissions, want of ordinary care, and the resulting Security Lapse—to wit, willfully, intentionally, recklessly, negligently, and knowingly selling and granting access to the PII of millions of U.S. citizens (*i.e.*, the "Class Members") to Ngo, a known identity thief, black market PII trafficker, and computer hacker, and his fraudster customers for several years—Defendant willfully and recklessly violated 15 U.S.C. § 1681(b), 15 U.S.C. § 1681a(d)(3), 15 U.S.C. § 1681b(a);(g), and 15 U.S.C. § 1681c(a)(6) (and the related applicable regulations) by failing to identify, implement, maintain and monitor the proper data security measures, policies, procedures, protocols, and software and hardware systems to safeguard and protect Plaintiffs' and Class Members' PII.

81. Defendant's above-described wrongful actions, inaction and omissions, and want of ordinary care, in turn, directly and proximately caused the Security Lapse which, in turn, directly and proximately resulted in the wrongful dissemination of Plaintiffs' and Class Members' PII into the public domain for no permissible purpose under FCRA. Defendant's above described

willful and reckless FCRA violations also have prevented it from timely and immediately notifying Plaintiffs and Class Members about the Security Lapse which, in turn, inflicted additional economic damages and other actual injury and harm on Plaintiffs and Class Members.

82. Defendant's above-described wrongful actions, inaction, omissions, and want of ordinary care, and the resulting Security Lapse, directly and proximately caused Plaintiffs and Class Members to suffer economic damages and other actual injury and harm, and collectively constitute the willful and reckless violation of FCRA. Had Defendant not engaged in such wrongful actions, inaction, omissions, and want of ordinary care, Plaintiffs' and Class Members' PII would not have been disseminated to the world for no permissible purpose under FCRA, and used to commit rampant identity fraud. Plaintiffs and Class Members, therefore, are entitled to declaratory relief (as set forth below), injunctive relief (as set forth below), and compensation for their economic damages, and other actual injury and harm in the form of, *inter alia,* (i) the lost intrinsic value of their privacy, (ii) deprivation of the value of their PII, for which there is a well-established national and international market, (iii) the financial and temporal cost of monitoring their credit, monitoring their financial accounts, and mitigating their damages, and (iv) statutory damages of not less than $100, and not more than $1000, each, under 15 U.S.C. § 1681n(a)(1).

83. Plaintiffs and Class Members also are entitled to recover punitive damages, under 15 U.S.C. § 1681n(a)(2), and their attorneys' fees, litigation expenses, and costs, under 15 U.S.C. § 1681n(a)(3).

COUNT II

NEGLIGENT VIOLATION OF THE FAIR CREDIT REPORTING ACT

(15 U.S.C. § 1681, *et seq.*)

84. The preceding factual statements and allegations are incorporated by reference.

85. In the alternative, by their above-described wrongful actions, inaction and omissions, want of ordinary care, and the resulting Security Lapse—to wit, selling and/or granting access to the PII of millions of U.S. citizens (*i.e.*, the "Class Members") to Ngo, a known identity thief, black market PII trafficker, and computer hacker, and his fraudster customers for several years—Defendant negligently or in a grossly negligent manner violated 15 U.S.C. § 1681(b), 15 U.S.C. § 1681a(d)(3), 15 U.S.C. § 1681b(a);(g), and15 U.S.C. § 1681c(a)(6) (and the related applicable regulations) by failing to identify, implement, maintain and monitor the proper data security measures, policies, procedures, protocols, and software and hardware systems to safeguard and protect Plaintiffs' and Class Members' PII.

86. Defendant's above-described wrongful actions, inaction and omissions, and want of ordinary care, in turn, directly and/or proximately caused the Security Lapse which, in turn, directly and proximately resulted in the wrongful dissemination of Plaintiffs' and Class Members' PII into the public domain for no permissible purpose under FCRA. Defendant's above-described willful and reckless FCRA violations also have prevented it from timely and immediately notifying Plaintiffs and Class Members about the Security Lapse which, in turn, inflicted additional economic damages and other actual injury and harm on Plaintiffs and Class Members.

87. It was reasonably foreseeable to Defendant that its failure to identify, implement, maintain and monitor the proper data security measures, policies, procedures, protocols, and software and hardware systems to safeguard and protect Plaintiffs' and Class Members' PII would result in a security lapse, whereby unauthorized third parties—*e.g.*, Ngo and his fraudster customers—would gain access to, and disseminate, Plaintiffs' and Class Members' PII into the public domain for no permissible purpose under FCRA.

///

88. Defendant's above-described wrongful actions, inaction, omissions, and want of ordinary care, and the resulting Security Lapse, directly and proximately caused Plaintiffs and Class Members to suffer economic damages and other actual injury and harm, and collectively constitute the negligent violation of FCRA. Had Defendant not engaged in such wrongful actions, inaction, omissions, and want of ordinary care, Plaintiffs' and Class Members' PII would not have been disseminated to the world for no permissible purpose under FCRA, and used to commit rampant identity fraud. Plaintiffs and Class Members, therefore, are entitled to declaratory relief (as set forth below), injunctive relief (as set forth below), and compensation for their economic damages, and other actual injury and harm in the form of, *inter alia*, (i) the lost intrinsic value of their privacy, (ii) deprivation of the value of their PII, for which there is a well-established national and international market, and (iii) the financial and temporal cost of monitoring their credit, monitoring their financial accounts, and mitigating their damages.

89. Plaintiffs and Class Members also are entitled to recover their attorneys' fees, litigation expenses, and costs, under 15 U.S.C. § 1681o(a)(2).

COUNT III

VIOLATION OF THE CALIFORNIA UNFAIR COMPETITION LAW

(CAL. BUS. & PROF. CODE §§ 17200, *et seq*.)

90. The preceding factual statements and allegations are incorporated by reference.

91. The California Unfair Competition Law, CAL. BUS. & PROF. CODE § 17200, *et seq*. ("UCL"), prohibits any "unlawful," "fraudulent," or "unfair" business act or practice and any false or misleading advertising, as those terms are defined by the UCL and relevant case law. Defendant engaged in unlawful, unfair and fraudulent practices, within the meaning of the UCL, by virtue of its above-described wrongful actions, inaction, omissions, want of ordinary care,

and the resulting Security Lapse.

92. In the course of conducting business, Defendant engaged in "unlawful" business practices, in violation of the UCL, by failing and refusing to safeguard and protect Plaintiffs' and Class Members' PII, and failing and refusing to, *inter alia*, (i) properly conduct its due diligence of CVI before acquiring it, (ii) thoroughly and completely investigate the Ngo identity fraud operation after obtaining full knowledge about Ngo and the substantial amount of money he sent CVI and Experian every month, (iii) notify Plaintiffs and Class Members about the Security Lapse, and (iv) provide Plaintiffs and Class Members with identity theft/identity fraud protection after promising Congress that it would do so. If Plaintiffs and Class Members had been notified in an appropriate fashion, they could have taken precautions to safeguard and protect their PII, finances, and identities. Defendant also engaged in "unlawful" business practices, in violation of the UCL, by profiting from the above-described illegal activities of Ngo and his fraudster customers who Defendant knew about (or should have known about sooner), and should have shut down sooner. Plaintiffs and Class Members reserve the right to allege other violations of law that constitute other unlawful business acts or practices. Such conduct is ongoing and continues to this date.

93. Defendant's above-described wrongful actions, inaction, omissions, want of ordinary care, misrepresentations, practices, non-disclosures, and the resulting Security Lapse also constitute "unfair" business acts and practices, within the meaning of CAL. BUS. & PROF. CODE § 17200, *et seq*., in that Defendant's conduct was (and continues to be) substantially injurious to consumers, offends public policy, is immoral, unethical, oppressive and unscrupulous, and the gravity of their wrongful conduct outweighs any alleged benefits attributable to such conduct. There were reasonably available alternatives to further Defendant's legitimate business interests other than the

above-described wrongful conduct.

94. The UCL also prohibits any "fraudulent business act or practice." Defendant's above-described inaction, omissions, and nondisclosures when it had a duty to speak were false, misleading and likely to deceive the consuming public, including Plaintiffs and Class Members, and violated the statute. Defendant's above-described wrongful actions, inaction, omissions, want of ordinary care, nondisclosures, and the resulting Security Lapse directly and proximately caused (and continue to cause) the above-described substantial economic damages and other injury and harm to Plaintiff and Class Members. Defendant systematically, repeatedly, voluntarily, and wrongfully disclosed Plaintiffs' and Class Members' confidential and sensitive PII, generating substantial profits in the process. Unless restrained and enjoined, Defendant will continue to engage in the above-described wrongful conduct.

95. Pursuant to CAL. BUS. & PROF. CODE § 17203, any person who engages, has engaged, or proposes to engage in "unlawful," "fraudulent," and/or "unfair" business acts or practices in violation of the UCL may be enjoined from such wrongful conduct. Accordingly, Plaintiffs, on behalf of themselves, Class Members, and the general public, seek an injunction against Defendant requiring Defendant to, *inter alia*, (i) notify each person whose PII (a) was accessed by Ngo and his fraudster customers, (b) was sold by Defendant to Ngo and his fraudster customers, or (c) was otherwise exposed in the Security Lapse, (ii) provide credit monitoring to each such person for at least three years, (iii) establish a fund (in an amount to be determined) to which such persons may apply for reimbursement of the time and out-of-pocket expenses they incurred to remediate identity theft and identity fraud (*i.e.*, data breach insurance), from July 1, 2010 forward to the date the above-referenced credit monitoring terminates, and (iv) discontinue its above-described wrongful actions, inaction, omissions, want of ordinary care, nondisclosures, and the resulting Security Lapse.

96. Plaintiffs and Class Members also are entitled to recover their attorneys' fees, expenses, and costs, under CAL. CODE CIV. P. § 1021.5; *Walker v. Countrywide Home Loans,* 98 Cal. App. 4th 1158, 1179 (Cal. Ct. App. 2002).

COUNT IV

DECLARATORY AND INJUNCTIVE RELIEF

97. The preceding factual statements and allegations are incorporated by reference.

98. Under the Declaratory Judgment Act, 28 U.S.C. § 2201, *et seq.*, the Court is authorized to enter a judgment declaring the Parties' rights and legal relations, and grant further necessary relief based upon such a judgment. The Court also has broad authority to restrain acts, such as here, that are tortious and violate the law.

99. An actual controversy has arisen in the wake of the Security Lapse regarding Defendants' duties to safeguard and protect Plaintiffs' and Class Members' confidential and sensitive PII. Defendant's PII security measures were (and continue to be) woefully inadequate. Plaintiffs and Class Members continue to suffer damages to their businesses and property, and other injury and harm as additional identity theft and identity fraud occurs.

100. **DECLARATORY RELIEF.** Pursuant to the Declaratory Judgment Act, Plaintiffs and Class Members request the Court to enter a judgment declaring, *inter alia*, (i) Defendant owed (and continues to owe) a legal duty to safeguard and protect Plaintiffs' and Class Members' confidential and sensitive PII, and timely notify them about the Security Lapse, (ii) Defendant breached (and continues to breach) such legal duties by failing to safeguard and protect Plaintiffs' and Class Members' confidential and sensitive payment PII, (iii) Defendant's breach of its legal duties directly and proximately caused the Security Lapse, and the resulting damages, injury, and harm suffered by Plaintiffs and Class Members, and (iv) Plaintiffs and Class Members are entitled

to the disgorgement of Defendant's gross revenues earned on such wrongful PII sales and the following injunctive relief.

101. **INJUNCTIVE RELIEF.** Defendant's above-described wrongful actions, inaction, omissions, want of ordinary care, nondisclosures, and the resulting Security Lapse have caused (and will continues to cause) Plaintiffs and Class Members to suffer irreparable harm in the form of, *inter alia*, economic damages and other injury and actual harm in the form of, *inter alia*, (i) actual identity theft and identity fraud, (ii) invasion of privacy, (iii) loss of the intrinsic value of their privacy, (iv) breach of the confidentiality of their consumer reports and PII, (v) deprivation of the value of their PII, for which there is a well-established national and international market, (vi) the financial and temporal cost of monitoring their credit, monitoring their financial accounts, and mitigating their damages, and (vii) the imminent, immediate, and continuing increased risk of ongoing identity theft and identity fraud. Such irreparable harm will not cease unless and until enjoined by this Court.

102. Plaintiffs and Class Members, therefore, are entitled to injunctive relief and other appropriate affirmative relief including, *inter alia*, an order compelling Defendant to, *inter alia*, (i) notify each person whose PII (a) was accessed by Ngo and/or his fraudster customers, (b) was sold by Defendant to Ngo and/or his fraudster customers, or (c) was otherwise exposed in the Security Lapse, (ii) provide credit monitoring to each such person for at least three years, (iii) establish a fund (in an amount to be determined) to which such persons may apply for reimbursement of the time and out-of-pocket expenses they incurred to remediate identity theft and/or identity fraud (*i.e.*, data breach insurance), from July 1, 2010 forward to the date the above-referenced credit monitoring terminates, (iv) refund (or disgorge) their gross revenue from transactions with Ngo and his fraudster customers involving Plaintiffs' and Class Members' PII and the earnings on such gross revenue, and (v) discontinue its above-described

wrongful actions, inaction, omissions, want of ordinary care, nondisclosures, and the resulting Security Lapse.

103. Plaintiffs and Class Members also are entitled to injunctive relief requiring Defendant to implement and maintain data security measures, policies, procedures, controls, protocols, and software and hardware systems, including, *inter alia*, (i) instituting policies and procedures for investigating and vetting customers for the PII in their possession, custody, and control, (ii) instituting policies and procedures for monitoring its customers and investigating any customers who conceivably may be using or re-selling such PII for improper purposes, (iii) engaging third-party security auditors/penetration testers and internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's computer systems on a periodic basis, (iv) engaging third-party security auditors and internal personnel to run automated security monitoring, (v) auditing, testing, and training its security personnel regarding any new or modified procedures, (vi) conducting regular database scanning and security checks, (vii) regularly evaluating web applications for vulnerabilities to prevent web application threats, and (viii) periodically conducting internal training and education to inform internal data security personnel how to identify and contain data security lapses.

104. If an injunction is not issued, Plaintiffs and Class Members will suffer irreparable injury in the event Defendant commits another security lapse, the risk of which is real, immediate, and substantial.

105. The hardship to Plaintiffs and Class Members if an injunction does not issue exceeds the hardship to Defendant if an injunction is issued. Among other things, if Defendant suffers another massive security lapse, Plaintiffs and Class Members will likely again incur millions of dollars in damages. On the other hand, and setting aside the fact that Defendant has a pre-existing legal obligation to employ adequate customer data security measures, Defendant's cost

to comply with the above-described injunction they are already required to implement is relatively minimal.

106. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another security lapse, thereby eliminating the damages, injury, and harm that would be suffered by Plaintiffs, Class Members, and the millions of consumers whose confidential and sensitive PII would be compromised.

TOLLING OF THE STATUTES OF LIMITATION

107. The preceding factual statements and allegations are incorporated by reference.

108. **FRAUDULENT CONCEALMENT.** Defendant took active steps to conceal its above-described wrongful actions, inaction, omissions, want of ordinary care, nondisclosures, and the resulting Security Lapse. The details of Defendant's efforts to conceal its above-described unlawful conduct are in its possession, custody, and control, to the exclusion of Plaintiffs, and await further discovery. When this material information was first revealed to Plaintiffs, they exercised due diligence by investigating the situation, retaining counsel, and pursuing their claims. Defendant fraudulently concealed its above-described wrongful conduct. Should such be necessary, therefore, all applicable statutes of limitation (if any) are tolled under the fraudulent concealment doctrine.

109. **EQUITABLE ESTOPPEL.** Defendant took active steps to conceal its above-described wrongful actions, inaction, omissions, want of ordinary care, nondisclosures, and the resulting Security Lapse. The details of Defendant's efforts to conceal its above-described unlawful conduct are in its possession, custody, and control, to the exclusion of Plaintiffs, and await further discovery. When this material information was first revealed to Plaintiffs, they exercised due diligence by investigating the situation, retaining counsel, and pursuing their claims. Defendant intentionally concealed its above-described wrongful conduct.

Should such be necessary, therefore, all applicable statutes of limitation (if any) are tolled under the doctrine of equitable estoppel.

110. **EQUITABLE TOLLING.** Defendant took active steps to conceal its above-described wrongful actions, inaction, omissions, want of ordinary care, nondisclosures, and the resulting Security Lapse. The details of Defendant's efforts to conceal its above-described unlawful conduct are in its possession, custody, and control, to the exclusion of Plaintiffs, and await further discovery. When this material information was first revealed to Plaintiffs, they exercised due diligence by investigating the situation, retaining counsel, and pursuing their claims. Defendant intentionally concealed its above-described wrongful conduct. Should such be necessary, therefore, all applicable statutes of limitation (if any) are tolled under the doctrine of equitable tolling.

PRAYER

WHERFORE, Plaintiffs, for themselves and Class Members, respectfully request that (i) Defendant be cited to appear and answer this lawsuit, (ii) this action be certified as a class action, (iii) Plaintiffs be designated the Class Representatives, and (iv) Plaintiffs' counsel be appointed as Class Counsel. Plaintiffs, for themselves and Class Members, further request that upon final trial or hearing, judgment be awarded against Defendant, in Plaintiffs' favor for:

(i) statutory and actual damages under the Fair Credit Reporting Act in an amount to be determined by the trier of fact;

(ii) punitive damages in an amount to be determined by the trier of fact;

(iii) declaratory and injunctive relief (as set forth above), including disgorgement of Defendant's gross revenue from transactions with Ngo and his fraudster customers involving Plaintiffs' and Class Members' PII and the earnings on such gross revenue;

(iv) attorneys' fees, litigation expenses and costs of suit incurred through the trial and any appeals of this case; and

(v) such other and further relief the Court deems just and proper.

JURY DEMAND

Plaintiffs, individually and on behalf of Class Members, respectfully demand a trial by jury on all of their claims and causes of action so triable.

Dated: July 17, 2015

BLOOD HURST & O'REARDON, LLP
TIMOTHY G. BLOOD (149343)
PAULA M. ROACH (254142)

By: *s/ Timothy G. Blood*
TIMOTHY G. BLOOD

701 B Street, Suite 1700
San Diego, CA 92101
Tel: 619/338-1100
619/338-1101 (fax)
tblood@bholaw.com
proach@bholaw.com

BARNOW AND ASSOCIATES, P.C.
BEN BARNOW
ERICH P. SCHORK
1 North LaSalle Street, Suite 4600
Chicago, IL 60602
Tel: 312/621-2000
312/641-5504 (fax)
b.barnow@barnowlaw.com
e.schork@barnowlaw.com

THE COFFMAN LAW FIRM
RICHARD L. COFFMAN
First City Building
505 Orleans St., Suite 505
Beaumont, TX 77701
Tel: 409/833-7700
866/835-8250 (fax)
rcoffman@coffmanlawfirm.com

Attornevs for Plaintiffs and the Putative Class