UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MISSOURI
EASTERN DIVISION

ANDREW DUQUM, individually and on behalf of all others similarly situated,

Plaintiff,

v.

SCOTTRADE, INC., a Missouri corporation,

Defendant.

[THIS DOCUMENT RELATES TO ALL CONSOLIDATED ACTIONS]

Case No. 4:15-cv-01537-SPM

CLASS ACTION

CONSOLIDATED CLASS ACTION COMPLAINT

Judge Shirley Padmore Mensah

JURY TRIAL DEMANDED

Plaintiffs Andrew Duqum, Stephen Hine, Matthew Kuhns, and Richard Obringer ("Plaintiffs"), individually and on behalf of all others similarly situated, bring this action against Defendant Scottrade, Inc. ("Scottrade").

INTRODUCTION

1. Scottrade is a financial brokerage and bank. To assist it in selling financial services, Scottrade collects a variety of confidential financial and other personal information from its customers. Its customers, including Plaintiffs and the other Class Members, reasonably expect and believe that Scottrade will take appropriate measures to protect their personal information. Meanwhile, Scottrade contractually obligates itself to using "industry leading security technologies" to protect its customers' information. For Plaintiffs and the other Class Members, Scottrade failed to live up to the expectations of its customers or its contractual and other obligations. As a result of Scottrade's failings, contact information, social security numbers, tax identification numbers, employer contact information, personal email addresses and other sensitive data (the "PII") of more than 4.6 million Scottrade customers was accessed, taken and used by a group of hackers. Scottrade's cybersecurity measures were so deficient that it never realized the massive theft occurred until two years later, when federal authorities told them about it. The hackers viewed and used the PII for a variety of schemes that resulted in the loss of millions of dollars.

2. Scottrade's databases were an easy target. As one of the hackers predicted, accessing Scottrade's database "will be a simple hit for us." The hacker was right. After obtaining the login credentials for one Scottrade account, from about September 2013 to about February 2014, the hackers were able to access and export the PII without detection

(the "Data Breach"), constituting an inexcusable failure of Scottrade's obligation to take reasonable steps to safeguard this information.

3. Scottrade owed a legal duty to Plaintiffs and the other Class members to maintain reasonable and adequate security measures to secure, protect, and safeguard the personal information stored on its network. Scottrade breached that duty by failing to design and implement appropriate firewalls and computer systems, failing to properly and adequately encrypt data, and unnecessarily storing and retaining Plaintiffs' and the other Class members' personal information on its inadequately protected network.

4. Scottrade was aware of its inadequate cybersecurity before the Data Breach, yet failed to appropriately safeguard the PII. Before the Data Breach, Scottrade's network had been hacked by criminals who used customer account information to conduct fraudulent stock trades. Before the Data Breach, government regulators had even levied fines against Scottrade because of its inadequate cybersecurity procedures and oversight. Nonetheless, Scottrade failed to take reasonable measures to safeguard the PII and never warned Plaintiffs and the other Class members that the information they provided to Scottrade was unreasonably susceptible to hackers. To the contrary, Scottrade promised it was adequately safeguarding the PII and contractually obligated itself to do so.

5. This action seeks to remedy these failings. Plaintiffs bring this action on behalf of themselves and persons whose personal or financial information was disclosed as a result of the data breach first disclosed by Scottrade on or about October 2, 2015.

6. Plaintiffs seek, for themselves and the Class, injunctive relief, actual and other economic damages, consequential damages, nominal damages or statutory damages, punitive damages, and attorneys' fees, litigation expenses and costs of suit.

VENUE AND JURISDICTION

7. This Court also has subject matter jurisdiction over this action pursuant to 28 U.S.C. §1332(d) because (a) there are 100 or more Class members, (b) at least one Class member is a citizen of a state that is diverse from Scottrade's citizenship, and (c) the matter in controversy exceeds $5,000,000, exclusive of interest and costs.

8. Venue is appropriate in this Court pursuant to 28 U.S.C. §1391 because Scottrade is headquartered in this district and a substantial part of the events or omissions giving rise to the claims occurred in this district.

PARTIES

9. At all relevant times, Plaintiff Andrew Duqum ("Duqum") has been a resident of the State of Missouri. Believing that Scottrade would safeguard his personal information, Mr. Duqum provided his PII to Scottrade in connection with his brokerage account opened near the end of 2013. Scottrade possessed, and currently possesses, Mr. Duqum's PII, which Scottrade was and is required to take reasonable steps to keep confidential. Mr. Duqum received an email from Scottrade confirming his PII was contained on and taken from Scottrade's databases between late 2013 and early 2014. Thereafter, one or more data thieves, and their subsequent customers or others coming into possession of the wrongfully disclosed PII, transferred, sold, opened, read, mined and otherwise used Mr. Duqum's PII, without his authorization, to their financial benefit and his financial and other detriment. Mr. Duqum has been charged and paid Scottrade fees in connection with his Scottrade account, a portion of which were used for data management and security pursuant to the contractual and other obligations of Scottrade.

10. At all relevant times, Plaintiff Stephen John Hine ("Hine") has been a resident of the State of California. Believing that Scottrade would safeguard his personal information, Mr. Hine provided his PII to Scottrade in connection with his two brokerage accounts opened in 2006. Scottrade possessed, and currently possesses, Mr. Hine's PII, which Scottrade was and is required to take reasonable steps to keep confidential. Mr. Hine received an email from Scottrade confirming his PII was contained on and taken from Scottrade's databases between late 2013 and early 2014. Thereafter, one or more data thieves, and their subsequent customers or others coming into possession of the wrongfully disclosed PII, transferred, sold, opened, read, mined and otherwise used Mr. Hine's PII, without his authorization, to their financial benefit and his financial detriment and other harm. Mr. Hine has been charged and paid Scottrade fees in connection with his Scottrade account, a portion of which were used for data management and security pursuant to the contractual and other obligations of Scottrade.

11. At all relevant times, Plaintiff Matthew Kuhns ("Kuhns") has been a resident of the State of Florida. Believing that Scottrade would safeguard his personal information, Mr. Kuhns provided his PII to Scottrade in connection with his brokerage account opened in 2005. Scottrade possessed, and currently possesses, Mr. Kuhns' PII, which Scottrade was and is required to take reasonable steps to keep confidential. Mr. Kuhns received an email from Scottrade confirming his PII was contained on and taken from Scottrade's databases between late 2013 and early 2014. Thereafter, one or more data thieves, and their subsequent customers or others coming into possession of the wrongfully disclosed PII, transferred, sold, opened, read, mined and otherwise used Mr. Kuhns' PII, without his authorization, to their financial benefit and his financial and other detriment. Mr. Kuhns has been charged

and paid Scottrade fees in connection with his Scottrade account, a portion of which were used for data management and security pursuant to the contractual and other obligations of Scottrade.

12. At all relevant times, Plaintiff Rick Obringer ("Obringer") has been a resident of the State of Nevada. Believing that Scottrade would safeguard his personal information, Mr. Obringer provided his PII to Scottrade in connection with his brokerage account opened between approximately 2002 and 2004. Although Mr. Obringer closed his Scottrade account in approximately 2008, Scottrade kept his PII, which Scottrade was and is required to take reasonable steps to keep confidential. Mr. Obringer received a letter postmarked October 28, 2015, from Scottrade confirming his PII was contained on and taken from Scottrade's databases between late 2013 and early 2014. Scottrade knew Mr. Obringer's account had been closed years earlier, but nonetheless did not bother to take basic steps to ensure it sent the required breach notification letter to Mr. Obringer's current address. Instead, Scottrade mailed the notice letter to an address from which Mr. Obringer moved in 2006. One or more data thieves, and their subsequent customers or others coming into possession of the wrongfully disclosed PII, transferred, sold, opened, read, mined and otherwise used Mr. Obringer's PII, without his authorization, to their financial benefit and his financial and other detriment. Mr. Obringer has been charged and paid Scottrade fees in connection with his Scottrade account, a portion of which were used for data management and security pursuant to the contractual and other obligations of Scottrade.

13. As a direct and proximate result of Scottrade's wrongful actions, inaction and/or omissions, the resulting Data Breach, and the resulting identity theft and identity fraud,[1] inflicted on Plaintiffs by one or more unauthorized third parties, Plaintiffs also have suffered (and will continue to suffer) economic damages and other injury and harm in the form of the deprivation of the value of their PII, for which there is a well-established national and international market. PII is a valuable property right. Faced with the choice of having their PII disclosed, compromised, transferred, sold, opened, read, mined and otherwise used without their authorization versus selling their PII on the black market and receiving the compensation themselves, Plaintiffs would choose the latter. Plaintiffs – not data thieves – should have the exclusive right to monetize their PII. Scottrade's wrongful actions, inaction and omissions, and the resulting Data Breach, deprived them of this right.

14. As a direct and proximate result of Scottrade's wrongful actions, inaction and/or omissions, the resulting Data Breach, and the resulting identity theft and identity fraud inflicted on them by one or more unauthorized third parties, Plaintiffs received a diminished value of the services they paid Scottrade to provide. A portion of the brokerage and financial service fees Plaintiffs paid was for data management and data security. Plaintiffs contracted for brokerage and financial services that included Scottrade's guaranty to safeguard and protect their PII, but instead, received financial and brokerage services lacking these important protections. Despite failing to implement or inadequately implementing policies to safeguard and protect Plaintiffs' PII, Scottrade has had the beneficial use and enjoyment of the full amount of such payments from Plaintiffs. Plaintiffs and Class members overpaid for Scottrade's services. Plaintiffs and

[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 (theft of government services, including medical services).

Class members did not receive the full benefit of their bargain, and instead received Scottrade's brokerage and/or financial services that were less valuable than what they paid for.

15. As a further direct and proximate result of Scottrade's wrongful actions, inaction and/or omissions, the resulting Data Breach, and the resulting identity theft and identity fraud inflicted on them by one or more unauthorized third parties, Plaintiffs have suffered (and will continue to suffer) other economic damages and injury and harm, including: (i) an imminent, immediate and the continuing increased risk of identity theft and identity fraud; (ii) invasion of privacy; (iii) breach of the confidentiality of their PII; (iv) deprivation of the value of their PII, for which there is a well-established national and international market; (v) failure to receive the full benefit of their bargain as a result of receiving brokerage and financial services that were less valuable than what they paid for; and/or (vi) the financial and/or temporal cost of monitoring their credit, monitoring their financial accounts, and mitigating their damages – for which they are entitled to compensation.

16. Defendant Scottrade is a Missouri corporation with its headquarters and principal place of business in Missouri. Scottrade is a privately owned discount retail brokerage firm headquartered in Town and Country, Missouri and does business in all fifty states.

PERSONAL IDENTIFICATION INFORMATION IS A VALUABLE PROPERTY RIGHT

17. At a FTC public workshop in 2001, then-Commissioner Orson Swindle described the value of a consumer's PII:

> The use of third party information from public records, information aggregators and even competitors for marketing has become a major facilitator of our retail economy.
>
> Even [Federal Reserve] Chairman [Alan] Greenspan suggested here some time ago that it's something on the order of the life blood, the free flow of

information.[2]

18. Though Commissioner Swindle's remarks are more than a decade old, their pertenance has increased over time, as PII functions as a "new form of currency" that supports a $26 billion per year online advertising industry in the United States.[3]

19. The FTC has also recognized that PII is a new – and valuable – form of currency. In a recent FTC roundtable presentation, another former Commissioner, Pamela Jones Harbour, underscored this point by observing:

> Most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis – and profit.[4]

20. Recognizing the high value that consumers place on their PII, many companies now offer consumers an opportunity to sell this information to advertisers and other third parties. The idea is to give consumers more power and control over the type of information that they share – and who ultimately receives that information. And by making the transaction transparent,

---

[2] Federal Trade Commission, *The Information Marketplace: Merging and Exchanging Consumer Data*, *Conference and Workshop*, *Washington D.C.*, 28 (March 13, 2011), *available at* https://www.ftc.gov/sites/default/files/documents/public_events/information-marketplace-merging-and-exchanging-consumer-data/transcript.pdf (last visited February 18, 2016).

[3] *See* J. Angwin and W. Steel, *Web's Hot New Commodity: Privacy*, The wall Street Journal, Feb. 28, 2001, *available at* http://online.wsj.com/article/SB10001424052748703529004576160764037920274.html (last visited August 8, 2015).

[4] Federal Trade Commission, *Statement of FTC Commissioner Pamela Jones Harbour* (Remarks Before FTC Exploring Privacy Roundtable), (Dec. 7, 2009), *available at* https://www.ftc.gov/public-statements/2009/12/remarks-ftc-exploring-privacy-roundtable (last visited February 18, 2016).

consumers will make a profit from the surrender of their PI.[5] This business has created a new market for the sale and purchase of this valuable data.[6]

21. Consumers place a high value not only on their PII, but also on the *privacy* of that data. Researchers have already begun to shed light on how much consumers value their data privacy – and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[7]

22. Notably, one study on website privacy determined that U.S. consumers valued the restriction of improper access to their PII – the very injury at issue here – between $11.33 and $16.58 per website.[8]

23. The United States Government Accountability Office noted in a June, 2007 report on Data Breaches ("GAO Report") that identity thieves use identifying data such as SSNs to open financial accounts, receive government benefits and incur charges and credit in a person's name.[9] As the GAO Report states, this type of identity theft is the most harmful because it may take time for the victim to become aware of the theft and can adversely impact the victim's credit rating.

---

[5] Steve Lohr, *You Want My Personal Data? Reward Me for It*, N.Y. Times, July 16, 2010, *available at* http://www.nytimes.com/2010/07/18/business/18unboxed.html?_r=0 (last visited February 18, 2016).

[6] *See* Julia Angwin and Emil Steel, *Web's Hot New Commodity: Privacy*, Wall Street Journal, Feb. 28, 2011, *available at* http://online.wsj.com/article/SB10001424052748703529004576160764037920274.html (last visited August 3, 2015).

[7] Janice Y. Tsai, et al., *The Effect of Online Privacy Information on Purchasing Behavior, An Experimental Study Information Systems Research* 22(2) 254, 254 (June 2011), available at http://www.guanotronic.com/~serge/papers/isr10.pdf (last visited February 18, 2016).

[8] II–Horn, Hann et al., *The Value of Online Information Privacy: An Empirical Investigation* (Mar. 2003) at table 3, *available at* http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.321.6125&rep=rep1&type=pdf (emphasis added) (last visited February 18, 2016).

[9] *See* http:///www.gao.gov/new.items/d07737.pdf.

24. In addition, the GAO Report states that victims of identity theft will face "substantial costs and inconveniences repairing damage to their credit records . . . [and their] good name."

25. According to the Federal Trade Commission ("FTC"), identity theft victims must spend countless hours and large amounts of money repairing the impact to their good name and credit record.[10] Identity thieves use personal information such as SSNs for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[11]

26. With access to an individual's sensitive information, criminals are capable of conducting many nefarious actions. Besides emptying the victim's bank account, identity thieves also commit various types of government fraud, such as: (1) obtaining a driver's license or official identification card in the victim's name but with the thief's picture; (2) using the victim's name and SSN to obtain government benefits; and/or, (3) filing a fraudulent tax return using the victim's information.

27. In addition, identity thieves may obtain a job using the victim's SSN, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.[12]

---

[10] *See* FTC Identity Theft Website: www.ftc.gov/bcp/edu/microsites/idtheft/consumers/about-identity-theft.html.

[11] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 CFR §603.2. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number. *Id*.

[12] *See* FTC Identity Theft Website, *supra*.

28. A person whose personal information has been compromised may not see any signs of identity theft for years. According to the GAO Report:

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

29. "PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets."[13] It is so valuable to identity thieves that once PII has been disclosed, criminals often trade it on the "cyber black-market" for several years. Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that PII has considerable market value.

30. Companies, in fact, also recognize PII and other sensitive information as an extremely valuable commodity akin to a form of personal property. For example, Symantec Corporation's Norton brand has created a software application that values a person's identity on the black market.[14] Likewise, in the wake of the Data Breach at issue, Scottrade's notice warned customers to be "particularly vigilant against email or direct mail schemes seeking to trick you into revealing personal information." According to Scottrade, "We understand how important information security and privacy are to you."[15]

31. As a result of its real value and the recent large-scale data breaches, identity thieves and cyber criminals have openly posted credit card numbers, SSNs, PII and other

---

13 *See 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) (citations omitted).

14 Risk Assessment Tool, Norton 2010, www.everyclickmatters.com/victim/assessment-tool.html.

15 https://www.scottrade.com/documents/pdf/osc.pdf

sensitive information directly on various Internet websites making the information publicly available. In one study, researchers found hundreds of websites displaying stolen PII and other sensitive information. Strikingly, none of these websites were blocked by Google's safeguard filtering mechanism – the "Safe Browsing list." The 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]

32. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' PII has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

33. It is within this context that Plaintiffs and the nearly 4.6 million customers of Scottrade who relied on Scottrade's Privacy and Security policies must now live with the knowledge that their personal information is forever in cyberspace and was taken by people willing to use the information for any number of improper purposes and scams, including making the information available for sale on the black-market.

SCOTTRADE FAILED TO HONOR ITS PROMISES TO KEEP SENSITIVE PERSONAL INFORMATION CONFIDENTIAL

34. Scottrade is a discount retail brokerage firm that became popular in the late 1990's during the dot.com bubble based on its low $7.00 online trading platform.

35. Scottrade provides both online and branch office services to its clients, including brokerage services, banking services, and retirement planning services for individuals and businesses.

---

16 http://www.stopthehacker.com/2010/03/03/the-underground-credit-card-blackmarket/

36. Scottrade's online trading website, the Scottrade Standard Trading Website, is used by millions of investors across the country to view their online statements for their brokerage and retirement accounts.

37. When a customer opens an account with Scottrade, he or she must complete the Brokerage Agreement, which, by its terms, incorporates Scottrade's Privacy Statement (the "Privacy Statement"), which becomes part of the contractual relationship between Scottrade and its customers.[17] Among other things Scottrade, collects names, addresses, phone numbers, social security numbers, work history and other personal identifying information.

38. The Privacy Statement explains not only when Scottrade collects customers' personal information (when customers open an account or provide account information, make a wire transfer, or make deposits or withdrawals from their accounts, as well as periodically through third parties such as credit bureaus, affiliates and other companies), but also what kinds of personal and financial information it collects and shares, including Social Security numbers and employment information, account balances and transaction history, and credit history and investment experience.[18]

39. Scottrade represents to customers, including via the Privacy Statement, and its Online Privacy Policy (described below) that it employs adequate safeguards to protect the personal identifying and financial information customers must provide to open an account.

40. For example, the Privacy Statement states that "[t]o protect your personal information from unauthorized access and use, we use security measures that comply with federal law. These measures include computer safeguards and secured files and buildings."[19]

---

17 https://www.scottrade.com/documents/alt/PrivacyStatement.pdf

18 *Id.*

19 *Id.*

41. According to Scottrade's Privacy Statement, Scottrade collects personal information from customers during the following types of activities:

> Open an account or provide account information • Give us your contact information or make a wire transfer • Make deposits or withdrawals from your account • We also collect your personal information from others, such as credit bureaus, affiliates or other companies.[20]

42. Scottrade's Online Privacy Policy repeats and reinforces the representations that it employs adequate, and in fact, "industry leading security technologies, including layered security and access controls over personal information" to safeguard its customer's personal information. In its Online Privacy Policy, Scottrade represents to its customers:

> **How We Protect Your Information**
>
> We comply with applicable laws and regulations regarding the protection of personal information. We maintain physical, electronic and procedural safeguards that restrict access to your personal information. We use industry leading security technologies, including layered security and access controls over personal information. These safeguards are reviewed as necessary and may be adjusted in response to advances in technology and the latest security threats or trends.
>
> Where we share personal information with a non-affiliated third party to assist us in providing financial services, we perform regular information security assessments to ensure that your personal information is protected. We also train our employees about privacy and our commitment to protect your personal information.[21]

43. Furthermore, in a document entitled "Secure Online Investing & Identity Theft Protection," which is available on Scottrade's website, Scottrade represents:

> **Take Control of Your Safety:**
>
> At Scottrade, we take security seriously and use a variety of measures to protect your personal information and accounts. We keep all customer information confidential and maintain strict physical, electronic and procedural safeguards to protect against unauthorized access to your information.

---

20 *Id*.

21 https://www.scottrade.com/disclosures/onlineprivacy.html (last accessed Feb. 17, 2016).

> Scottrade is committed to constantly updating its practices to stay ahead of identity thieves. Using **VeriSign Identity Protection Fraud Detection Service**, for example, Scottrade automatically checks your account for signs of activity from a foreign computer.[22]

44. Indeed, Scottrade recognizes that "[a]ccount numbers, Social Security numbers and other pieces of personal information can all be used to commit fraud."

45. Plaintiffs and Class members bargained for, and expected to receive, data security measures safeguarding and protecting the privacy of their sensitive personal identifying and financial information when they opened accounts with Scottrade and relied on Scottrade's representations regarding its data security measures in opening their accounts.

46. Plaintiffs would not have opened accounts with Scottrade, or would not have paid as much with respect to those accounts, had they known that Scottrade failed to take reasonable precautions to secure their personal identifying information and financial data.

47. At all times relevant, Scottrade was obligated to comply with the terms of its own privacy policy, in accordance with the promises it uniformly made to Plaintiffs and the Class. Plaintiffs and the Class bargained for the privacy and security of their information during the sign up process and through their customer agreement with Scottrade. Security of one's personal and financial data is central to the reasonable customer's decision to invest with Scottrade and provide them with their private and sensitive PII.

---

22 https://www.scottrade.com/online-brokerage/secure-trading.html

THE 2013-2014 SCOTTRADE DATA BREACH IS FIRST DISCLOSED 16-24 MONTHS AFTER IT OCCURRED

48. On October 2, 2015, Bryan Krebs of "Krebs On Security" published an article alerting readers to the fact that Scottrade had just disclosed a breach involving confidential information of 4,600,000 million customers.[23]

49. Mr. Krebs reported that an email was sent to customers of Scottrade that day stating that Scottrade had been the victim of cyber security crimes involving the theft of information from Scottrade and other financial service companies.[24]

50. According to Mr. Krebs:

> "In an email sent today to customers, St. Louis-based Scottrade said it recently heard from federal law enforcement officials about crimes involving the theft of information from Scottrade and other financial services companies.
>
> 'Based upon our subsequent internal investigation coupled with information provided by the authorities, we believe a list of client names and street addresses was taken from our system,' the email notice reads. 'Importantly, we have no reason to believe that Scottrade's trading platforms or any client funds were compromised. All client passwords remained encrypted at all times and we have not seen any indication of fraudulent activity as a result of this incident.'
>
> The notice said that although Social Security numbers, email addresses and other sensitive data were contained in the system accessed, 'it appears that contact information was the focus of the incident.' The company said the unauthorized access appears to have occurred over a period between late 2013 and early 2014."

51. Mr. Krebs contacted Scottrade spokesperson Shea Leordeanu to inquire about the context of the notification from federal law enforcement officials concerning the actual date of the breach. In response, Ms. Leordeanu said the company couldn't comment on the incident

---

23 http://krebsonsecurity.com/2015/10/scottrade-breach-hits-4-6-million-customers/

24 *Id*.

much more in the information included in its website notice about the attack.[25] She did, however, state that "Scottrade learned about the date of theft from the FBI, and the company is working with agents from FBI field offices in Atlanta and New York."[26]

52. Mr. Krebs surmised that the intent of the intruders may have been to obtain Scottrade user data to facilitate stock scams, much like the J.P. Morgan Chase breach.

53. Numerous online news sites reported that there may be a connection between the Scottrade attack and the 2014 J.P. Morgan Chase hack, which involved the exposure of the contact information of more than 76 million consumers.[27] As later confirmed, these reports were correct.

54. The authorities have alleged that the email addresses were taken from J.P. Morgan Chase for the purpose of implementing stock manipulation schemes involving emails to pump penny stocks.

55. As with Scottrade, according to the New York Times, the J.P. Morgan breach could have been prevent. In fact, it is detailed in the December 22, 2014 article:

> "Most big banks use a double authentication scheme, known as two-factor authentication, which requires a second one-time password to gain access to a protected system. But JPMorgan's security team had apparently neglected to upgrade one of its network servers with the dual password scheme, the people briefed on the matter said. That left the bank vulnerable to intrusion.
>
> …
>
> The revelation that a simple flaw was at issue may help explain why several other financial institutions that were targets of the same hackers were not ultimately affected nearly as much as JPMorgan Chase was. To date, only two other institutions have suffered some kind of intrusion, but those breaches were said to be relatively minor by people briefed on the attacks.

---

25 *Id.*

26 *Id.*

27 http://fortune.com/2015/10/02/scottrade-data-breach/

> What is clear is JPMorgan's attack did not involve the use of a so-called zero day attack – the kind of sophisticated, completely novel software bug that can sell for a million dollars on the black market. Nor did hackers use the kind of destructive malware that government officials say hackers in North Korea used to sabotage data at Sony Pictures.
>
> …
>
> It is not clear why the vulnerability in the bank's network had gone unaddressed previously. But this summer's hack occurred during a period of high turnover in the bank's cybersecurity team with many departing for First Data, a payments processor."[28]

56. More troubling about the news that the attack may have been an attempt to obtain client information for the intent of manipulating security stock prices is the fact that Scottrade has been fined and publically reprimanded on several occasions for failing to comply with industry standards regarding network security, as well as failing to maintain proper supervisory mechanisms involving wire transfers:[29]

> "FINRA also found that Scottrade failed to establish a reasonable supervisory system to monitor for wires to third-party accounts. From October 2011 to October 2013, Scottrade failed to obtain any customer confirmations for third-party wire transfers of less than $200,000, and Scottrade failed to ensure that the appropriate personnel obtained confirmations for third-party wire transfers of between $200,000 and $500,000.
>
> During that period, the firm processed more than 17,000 third-party wire transfers totaling more than $880 million.
>
> "Firms must have robust supervisory systems to monitor and protect the movement of customer funds," Brad Bennett, executive vice president and chief of enforcement, said in a statement. "Morgan Stanley and Scottrade had been alerted to significant gaps in their systems by FINRA staff, yet years went by before either firm implemented sufficient corrective measures."
>
> Both firms were cited for the weak supervisory systems by FINRA examination teams in 2011, but neither took necessary steps to correct the supervisory gaps."

---

[28] http://dealbook.nytimes.com/2014/12/22/entry-point-of-jpmorgan-data-breach-is-identified/

[29] http://www.thinkadvisor.com/2015/06/22/morgan-stanley-scottrade-fined-by-finra-for-failin

57. Moreover, Scottrade suffered another data breach in May 2014. According to MarketWatch.com, dated October 9, 2014, a "Russian national living in New York, Petr Murmylyuk, was sentenced to 30 months in prison in January 2014 for hacking into retail brokerage accounts and making unauthorized trades from online accounts at Scottrade, E*Trade Financial, Fidelity Investments, Charles Schwab and other brokerages. He and his co-conspirators made trades in victim accounts to move the prices of holdings in accounts they had opened using stolen identities, causing about $1 million in losses, according to the Federal Bureau of Investigation."[30]

THE DEPARTMENT OF JUSTICE REVEALS THE SCOPE OF THE SCOTTRADE DATA BREACH

58. On November 10, 2015, the DOJ unsealed two indictments revealing the Scottrade data breach was part of a scheme to hack Scottrade and other financial institutions with large customer databases. According to the indictment, the four hackers used the PII taken from Scottrade for various unlawful business enterprises.

59. During at least in or about September 2013 to in or about February 2014, the hackers gained access to Scottrade's network, including Scottrade's customer databases. The hackers exported and used the confidential PII.

60. In or about October 2012, hacker Joshua Samuel Aaron provided login credentials for a Scottrade account to hacker Gery Shalon. Using the login credentials from just a single Scottrade account, the Scottrade hackers were able to gain access to Scottrade's internal enterprise networks.

[30] http://www.marketwatch.com/story/was-your-brokerage-account-hacked-heres-how-to-know-2014-07-25

61. Once inside Scottrade's networks, the hackers had the ability to move from application to application until they found the sensitive data they desired. The hackers discussed the PII visible on the Scottrade database and exported the PII to anonymous overseas servers setup by one of the hackers.

62. The hackers took the PII for the purpose of building their own competing customer database for marketing and brokering stock transactions.

63. The hackers went through the process of cleaning up and reformatting the PII and then generated reports from it.

64. The information was readily available, even surprising the hackers. For example, on or about September 5, 2013, hacker John Doe told hacker Shalon in an online chat that he "found passwords to scottrade.com on VPN." Hacker Shalon responded, "wow…Seriously?"

65. On or about September 8, 2013, hacker John Doe told hacker Shalon in an online chat that he was still working and "need[ed] to pick open scottrade." Hacker Shalon replied, "It will give us a very big push!" Hacker Shalon explained to hacker John Doe that they were looking for "investors' databases….The investors are looking for ways to make money….And we give them ways to make money."

66. On or about November 19, 2013, hacker John Doe told hacker Shalon in an online chat, "I am working on scottrade, I am trying to get in there. Seems to be working." Hacker Shalon responded, "[y]es it will be a simple hit for us."

67. On or about November 22, 2013, hacker John Doe told hacker Shalon in an online chat that he was "browsing inside the [Scottrade] network now, looking for a database."

68. On or about November 23, 2013, hacker Shalon provided hacker John Doe with login credentials for a Scottrade account. According to the DOJ indictment, less than an hour

after thanking hacker Shalon for providing login credentials, hacker John Doe located Scottrade's customer database and reported to Hacker Shalon in an online chat, "6 mil users there approx."

69. On or about the next day, hacker Shalon replied, "Fuck that's a shitload :)," and asked what data fields were visible. Hacker John Doe provided a full list of data fields in Scottrade's confidential customer database, including names, email addresses, residential addresses, and phone numbers.

70. On or about November 23, 2013, the hackers uploaded four files containing customer PII taken from Scottrade's database.

71. On or about November 25, 2013, hacker John Doe told hacker Shalon in an online chat that Scottrade also had a bank database, and hacker Shalon asked, "can we get it?" Hacker John Doe reported to hacker Shalon that he uploaded data for approximately 200,000 to 300,000 bank customers for hacker Shalon in a file.

72. On or about November 27, 2013, hacker John Doe reported he took additional customer data from Scottrade.

73. The hackers set up dozens of shell companies and used fake passports and other fraudulent credentials to maintain false identities.

74. The hackers used the PII to operate a stock price manipulation scheme that amassed millions of dollars. They also operated a dozen illegal Internet gambling websites, and a Bitcoin exchange that generated millions more, according to authorities.

SCOTTRADE'S NOTIFICATION OF THE 2-YEAR OLD DATA BREACH AND OFFERED "REMEDY" ARE INADEQUATE AND CREATE A BURDEN ON THE AFFECTED CUSTOMERS

75. In breach of its duties, Scottrade's security measures were not even sufficient to detect the hack, let alone prevent or minimize it. Until the federal government stepped in, Scottrade was unaware of the massive data breach.

76. The FBI notified Scottrade of the Data Breach in August 2015.

77. On approximately September 25, 2015, the FBI notified Scottrade that it could inform its customers about the Data Breach. Nevertheless, even then Scottrade waited an additional week to begin doing so.

78. On October 2, 2015, possibly forced by media accounts of the breach, Scottrade began notifying Plaintiffs and Class Members about the Data Breach via email or mail, confirming the security breach of their personal and private information – that Scottrade received from them during the course of their investment relationship – including, but not limited to: (i) names; (ii) addresses; (iii) Social Security numbers; (iv) employers' names; and (v) tax identification numbers.

79. Many affected customers will not receive the Data Breach notice. For example, affected customers may have changed email or mailing addresses, or used alternative email addresses for personal and financial matters. Scottrade could have sent text messages, like J.P. Morgan Chase and other banks use to instantly notify customer of a fraud alert of breach of their secured account, but instead chose to send only an email or letter.

80. The Data Breach notice is materially misleading and does not fully disclose to Scottrade customers the scope of the ongoing threat.

81. For example, Scottrade vaguely advised the recipients of the notice that their personal information "*may* have been compromised" in 2013 through 2014. Scottrade also stated that it is not aware which specific personal customer information was actually taken during the Data Breach, but, according to Scottrade, "it appears contract information was the focus of the incident." The database accessed, however, contains, among other things, Social Security numbers, email addresses and other "***sensitive data***" (which is not defined in the Data Breach notice). It is highly unlikely that the criminal hackers, having access to the above information, would only take the affected customer's name and email address.

82. The Data Breach notice also failed to explain the breadth of the Data Breach and the potential threat that customer's face. For example, the number of customers affected is not listed in the notice, nor are there any disclosures about how the breach occurred or why their customer's personal information was not properly safeguarded and protected:

> "Federal law enforcement officials recently informed us that they've been investigating cybersecurity crimes involving the theft of information from Scottrade and other financial services companies. We immediately initiated a comprehensive response.
>
> Based upon our subsequent internal investigation coupled with information provided by the authorities, we believe a list of client names and street addresses was taken from our system. Importantly, we have no reason to believe that Scottrade's trading platforms or any client funds were compromised. All client passwords remained encrypted at all times and we have not seen any indication of fraudulent activity as a result of this incident.
>
> Although Social Security numbers, email addresses and other sensitive data were contained in the system accessed, it appears that contact information was the focus of the incident.
>
> The unauthorized access appears to have occurred over a period of several months between late 2013 and early 2014. We have secured the known intrusion point and conducted an internal data forensics investigation on this incident with assistance from a leading computer security firm. We have taken appropriate steps to further strengthen our network defenses."

83. The Data Breach notice also squarely placed the burden on Plaintiffs and the Class, rather than Scottrade, to protect themselves and mitigate their data breach damages. Scottrade instructed its customers to review their account statements, monitor their credit reports, and obtain fraud alerts:

> "As always, we encourage you to regularly review your Scottrade and other financial accounts and report any suspicious or unrecognized activity immediately. As recommended by federal regulatory agencies, you should remember to be vigilant for the next 12 to 24 months and report any suspected incidents of fraud to us or the relevant financial institution. Please also read the important information included on ways to protect yourself from identity theft.
>
> We encourage clients to be particularly vigilant against email or direct mail schemes seeking to trick you into revealing personal information. Never confirm or provide personal information such as passwords or account information to anyone contacting you. Please know that Scottrade will never send you any unsolicited correspondence asking you for your account number, password or other private information. If you receive any letter or email requesting this information, it is fraudulent and we ask that you report it to us at phishing@scottrade.com. Be cautious about opening attachments or links from emails, regardless of who appears to have sent them."

84. The Data Breach notice states that Scottrade will provide one year of credit monitoring and identity theft insurance to affected persons. The offered "credit monitoring," however, is inadequate and requires affected customers to spend additional time and resources, including time filling out forms, and making phones calls to obtain full coverage:

> We have arranged to have AllClear ID help you protect your identity for one year at no cost to you, effective Oct. 2, 2015. You are pre-qualified for AllClear SECURE identity repair and protection services and have additional credit monitoring options available with AllClear PRO, also at no cost to you.
>
> AllClear SECURE: The team at AllClear ID is ready and standing by if you need identity repair assistance. This service is automatically available to you with no enrollment required. If a problem arises, simply call 855.229.0083 and a dedicated investigator will do the work to recover financial losses, restore your credit and make sure your identity is returned to its proper condition.
>
> AllClear PRO: This service offers additional layers of protection including credit monitoring and a $1 million identity theft insurance policy. To use the PRO service, you will need to provide your personal information to AllClear ID. You

> may sign up online at https://scottrade.allclearid.com or by phone by calling 855.229.0083.
>
> This hotline is available from 8:00 am to 8:00 pm (central) Monday through Saturday.
>
> Please note: Additional steps may be required by you in order to activate your phone alerts and monitoring options.

85. The one-year credit monitoring offered by Scottrade also does not provide comprehensive protection to the affected customers. Scottrade does not disclose this important fact. For example, the limited one-year offer does not include monitoring the online black market for identity theft.

86. Many of Scottrade's other mitigation suggestions also require Plaintiffs and Class to incur additional time and out-of-pocket expenses to protect themselves from the Data Breach.

> Review Your Accounts and Credit Reports
>
> Regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies.
>
> You may obtain a free copy of your credit report online at www.annualcreditreport.com by calling toll-free 1.877.322.8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service. P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed below.
>
> - Equifax, P.O. Box 740241, Atlanta, Georgia 30374-0241. 1.800.685.1111. www.equifax.com
> - Experian, P.O. Box 9532, Allen, TX 75013, 1.888.397.3742. www.experian.com
> - TransUnion, 2 Baldwin Place, P.O. Box 1000, Chester, PA 19016. 1.800.916.8800.www.transunion.com

87. Scottrade's Data Breach notice also states "You may wish to consider contacting the fraud department of the three major credit bureaus to request a 'fraud alert' be placed on your file." Scottrade's Data Breach notice does not disclose the important fact that because the theft occurred two years ago a fraud alert is not likely effective. Moreover, Scottrade's Data Breach

notice does not disclose that a fraud alert may not prevent the misuse of existing accounts, and for that reason the Federal Trade Commission still recommends "You still need to monitor all bank, credit card and insurance statements for fraudulent transactions."[31]

88. Scottrade's Data Breach notice also states "You may wish to request a security freeze on your credit reports." As a general rule, the fee to place a "security freeze" on one's credit report, as suggested by the Data Breach notice, is approximately $5-$10 each time it is placed at each of the three credit reporting agencies (Experian, Equifax, and TransUnion). Thereafter, in order to allow anyone check your credit, there is also an associated fee each time to lift the freeze. Moreover, if an identify thief has already used data to open accounts, then a credit freeze will not provide any benefits. A credit freeze also does not prevent identity thieves from making changes to existing accounts.

89. Monitoring one's credit reports, another option suggested by the Data Breach notice, would cause an affected Scottrade customer to incur an expense to see his or her credit reports beyond the one free annual report to which they are entitled.

90. Affected customers are also instructed to place fraud alerts. Because Scottrade let the Data Breach go undetected for two years, a fraud alert may not be useful. Scottrade does not disclose this important fact. Furthermore, placing fraud alerts also costs Scottrade's customers additional money and time:

> Consider Placing a Fraud Alert
>
> You may wish to consider contacting the fraud department of the three major credit bureaus to request that a "fraud alert" be placed on your file. A fraud alert notifies potential lenders to verify your identification before extending credit in your name.

---

31 http://www.consumer.ftc.gov/articles/0497-credit-freeze-faqs

91. Scottrade has never advised customers to change their account passwords. To the contrary, Scottrade's Data Breach notice informed customers "all client passwords remained encrypted at all times." This statement is vague, misleading, and provides Scottrade's customers with a false sense of security. Encryption is not an iron-clad promise, particularly where, as here, the thieves perpetrate a series of data breaches and have boasted and demonstrated that they will use the information for their wide variety of unlawful business ventures. Accordingly, security strategists believe Scottrade customers should perform a careful review of their account records, and change their password" on both the Scottrade website and any other websites where they may have used the same credentials.[32]

92. Although Scottrade know about the vulnerabilities of its online network and lack of internal supervisory mechanisms, Scottrade continued to represent and promise that client's personal and private information was safe and secure.

93. At all relevant times, Scottrade designed and implemented its policies and procedures regarding the security of protected financial information and sensitive information. These policies and procedures failed to adhere to reasonable and best industry practices in safeguarding protected health information and other sensitive information.

94. As customers of Scottrade, Plaintiffs and the Class members provided Scottrade with their PII, as required under their service agreements with Scottrade. Plaintiffs and Class members relied on Scottrade to keep their sensitive information safeguarded and otherwise confidential.

---

[32] http://www.eweek.com/security/scottrade-misses-breach-until-notified-by-fbi-2-years-later.html; http://arstechnica.com/security/2015/10/scottrade-breach-exposes-sensitive-data-for-4-6-million-customers/

95. Scottrade's wrongful actions, inaction, omissions, and want of ordinary care in failing to completely and accurately notify Plaintiffs and the Class about the data breach and corresponding unauthorized release and disclosure of their personal information was arbitrary, capricious and in derogation of Scottrade's duties to Plaintiffs and the Class.

CLASS ALLEGATIONS

96. Pursuant to Rule 23(b)(1), (b)(2), (b)(3), and (c)(4) of the Federal Rules of Civil Procedure, Plaintiffs bring this class action lawsuit on behalf of themselves and all other members of the Class (the "National Class") defined as follows:

> All persons in the United States whose personal or financial information was compromised as a result of the data breach first disclosed by Scottrade on or about October 2, 2015.

97. In addition to the National Class, pursuant to Rule 23(b)(1), (b)(2), (b)(3), and (c)(4) of the Federal Rules of Civil Procedure, Plaintiffs seek certification of a "Multistate Class" defined as follows:

> All persons in the Consumer Fraud States[33] whose personal or financial information was compromised as a result of the data breach first disclosed by Scottrade on or about October 2, 2015.

98. In the alternative to the Multistate Class, pursuant to Rule 23(b)(1), (b)(2), (b)(3), and (c)(4) of the Federal Rules of Civil Procedure, Plaintiffs seek certification of separate California, Florida, Missouri, and Nevada classes defined as follows:

> All persons in California whose personal or financial information was compromised as a result of the data breach first disclosed by Scottrade on or about October 2, 2015. (the "California Class")

---

[33] States with similar consumer fraud laws as applied to the facts of this case include California (Cal. Bus. & Prof. Code §17200, *et seq.* and Cal. Civil Code §1750, *et seq.*); Florida (Fla. Stat. §501.201, *et seq.*); Illinois (815 ICLS §505/1, *et seq.*); Massachusetts (Mass. Gen. Laws Ch. 93A, *et seq.*); Michigan (Mich. Comp. Laws §445.901, *et seq.*); Minnesota (Minn. Stat. §325F.67, *et seq.*); Missouri (Mo. Rev. Stat. §407.010, *et seq.*); New Jersey (N.J. Stat. §56:8-1, *et seq.*); New York (N.Y. Gen. Bus. Law §349, *et seq.*); and Washington (Wash. Rev. Code §19.86.010, *et seq.*).

All persons in Florida whose personal or financial information was compromised as a result of the data breach first disclosed by Scottrade on or about October 2, 2015. (the "Florida Class")

All persons in Missouri whose personal or financial information was compromised as a result of the data breach first disclosed by Scottrade on or about October 2, 2015. (the "Missouri Class")

All persons in Nevada whose personal or financial information was compromised as a result of the data breach first disclosed by Scottrade on or about October 2, 2015. (the "Nevada Class")

99. The California Class, Florida Class, Missouri Class, and Nevada Class are the "Single-State Classes."

100. The National Class, together with the Multistate Class, and Single-State Classes are collectively referred to as the Classes.

101. Excluded from the Classes are: (1) Scottrade and its officers, directors, employees, principals, affiliated entities, controlling entities, agents, and other affiliates; (2) the agents, affiliates, legal representatives, heirs, attorneys at law, attorneys in fact, or assignees of such persons or entities described herein; and (3) the Judge(s) assigned to this case and any members of their immediate families.

102. **Numerosity.** Scottrade is one the largest brokerages in the country. While the exact number of Class members are unknown, Scottrade has admitted the personal information, including names, mailing addresses, phone numbers, and email addresses of approximately 4,600,000 million customers was taken during the Data Breach. Plaintiffs therefore believe that the Class is so numerous that joinder of all members is impractical.

103. **Typicality.** Plaintiffs' claims are typical of the claims of the Class. Plaintiffs and the Class members were injured by the same wrongful acts, practices, and omissions committed

by Scottrade, as described herein. Plaintiffs' claims therefore arise from the same practices or course of conduct that give rise to the claims of all Class members.

104. **Commonality.** Common questions of law and fact exist as to all Class members and predominate over any individual questions. Such common questions include, but are not limited to:

A. Whether Scottrade has engaged in unlawful, unfair or fraudulent business acts or practices;

B. Whether Scottrade has engaged in the wrongful conduct alleged herein;

C. Whether Scottrade used reasonable or industry standard measures to protect Class members' personal and financial information;

D. Whether Scottrade adequately or properly segregated its network so as to protect personal customer data;

E. Whether Scottrade knew or should have known prior to the security breach that its network was susceptible to a potential data breach;

F. Whether Scottrade should have notified the Class that it failed to use reasonable and best practices, safeguards, and data security measures to protect customers' personal and financial information;

G. Whether Scottrade should have notified Class members that their personal and financial information would be at risk of unauthorized disclosure;

H. Whether Scottrade intentionally failed to disclose material information regarding its security measures, the risk of data interception, and the ongoing Data Breach;

I. Whether Scottrade's acts, omissions, and nondisclosures were intended to deceive Class members;

J. Whether Scottrade's conduct violated the laws alleged;

K. Whether Plaintiffs and the Class members are entitled to restitution, disgorgement, and other equitable relief; and

L. Whether Plaintiffs and the Class members are entitled to recover actual damages, statutory damages, and punitive damages.

105. **Adequacy.** Plaintiffs will fairly and adequately protect the interests of the Class members. Plaintiffs are adequate representatives of the Class in that they have no interests which are adverse to or conflict with those of the Class members Plaintiffs seek to represent. Plaintiffs have retained counsel with substantial experience and success in the prosecution of complex consumer protection class actions of this nature.

106. **Superiority.** A class action is superior to any other available method for the fair and efficient adjudication of this controversy since individual joinder of all Class members is impractical. Furthermore, the expenses and burden of individual litigation would make it difficult or impossible for the individual members of the Class to redress the wrongs done to them, especially given that the damages or injuries suffered by each individual member of the Class may be relatively small. Even if the Class members could afford individualized litigation, the cost to the court system would be substantial and individual actions would also present the potential for inconsistent or contradictory judgments. By contrast, a class action presents fewer management difficulties and provides the benefits of single adjudication and comprehension supervision by a single court.

COUNT I

Breach of Contract
(On Behalf of Plaintiffs and the National Class, or Alternatively, Each of the Single-State Classes)

107. Plaintiffs re-allege and incorporate by reference Paragraphs 1-106 as if fully set forth herein.

108. When Plaintiffs and Class members provided their personal and financial information to Scottrade in order to receive the company's services, they entered into express contracts with Scottrade pursuant to which Scottrade agreed to safeguard and protect such information from being compromised.

109. Scottrade solicited Plaintiffs and Class members to sign up with Scottrade and to provide their personal and financial information. Plaintiffs and Class members later paid money to Scottrade based on Scottrade's express representations concerning the safeguarding and protection of personal information.

110. Plaintiffs and Class members fully performed their obligations under the contracts with Scottrade.

111. Scottrade breached the contracts, including because it did not comply with applicable laws and regulations as described herein or otherwise adequately safeguard or protect Plaintiffs' and the proposed Class members' personal data from being accessed and taken. Scottrade did not maintain sufficient security measures and procedures to prevent unauthorized access to Plaintiffs' and the Class members' personal and financial information.

112. Plaintiffs and Class members had their personal and financial information compromised as a result of the Data Breach.

113. Plaintiffs and the Class members have suffered and will continue to suffer damages as the result of Scottrade's breach, including the monetary fees that Plaintiffs and Class members paid to Scottrade.

114. The losses and damages sustained by Plaintiffs and Class members as described herein were the direct and proximate result of Scottrade's breaches of the contracts between it and Plaintiffs and Class members.

COUNT II

Breach of Implied Contract
(In the Alternative to Count I, and on Behalf of Plaintiffs and the National Class, or Alternatively, Each of the Single-State Classes)

115. Plaintiffs re-allege and incorporate by reference Paragraphs 1-106 as if fully set forth herein.

116. Plaintiffs bring this cause of action in the alternative to Count I, and to the extent that an express contract is not found to exist between Scottrade on the one hand, and Plaintiffs and Class members on the other.

117. When Plaintiffs and Class members provided their personal and financial information to Scottrade in order to receive the company's services, they entered into implied contracts with Scottrade pursuant to which Scottrade agreed to safeguard and protect such information from being compromised.

118. Scottrade solicited Plaintiffs and Class members to sign up with Scottrade and to provide their personal and financial information. Plaintiffs and Class members accepted Scottrade's offer and provided their personal and financial information. Plaintiffs and Class members paid money to Scottrade to protect and safeguard their personal information and confidentiality.

119. Plaintiffs and Class members would not have provided and entrusted their financial and personal information to Scottrade in the absence of the implied contracts.

120. Plaintiffs and Class members fully performed their obligations under the implied contracts with Scottrade.

121. In the contracts, Scottrade promised to use industry leading measures to safeguard and protect Plaintiffs' and Class members' PII.

122. Scottrade breached the implied contracts and did not take reasonable measures to safeguard or protect Plaintiffs' and the proposed Class members' PII. Scottrade did not maintain sufficient security measures and procedures to prevent unauthorized access to Plaintiffs' and the Class members' personal and financial information.

123. Scottrade's failure to fulfill their implied contractual obligations resulted in Plaintiffs and the Class members PII being taken and receiving services of far less value than what was promised, *i.e.*, services that included adequate protection of confidential information. Accordingly, Plaintiffs and the Class members did not receive the full benefit of their bargain.

124. Plaintiffs and the Class members have suffered and will continue to suffer damages as the result of Scottrade's breach, including the monetary difference between the amount paid for services as promised (which were promised to include adequate data protection) and the services actually provided by Scottrade (which did not include adequate data protection).

125. The losses and damages sustained by Plaintiffs and Class members as described herein were the direct and proximate result of Scottrade's breaches of the implied contracts between it and Plaintiffs and Class members.

COUNT III

Negligence
(On Behalf of Plaintiffs and the National Class, or Alternatively, the Single-State Classes)

126. Plaintiffs re-allege and incorporate by reference Paragraphs 1-106 as if fully set forth herein.

127. During the course of conducting its business, Scottrade collected customers' PII. It was reasonably foreseeable that third parties would attempt to acquire such information given the risk and frequency of security breaches, including the breach that occurred in 2014 involving a Russian national, prior security alerts, and the potential fraudulent and criminal uses of the information if acquired, among other things.

128. In addition, Scottrade had notice of a possible security breach due to the prior targeting of other large retailers and financial institutions, including itself, by third parties seeking such information.

129. Consequently, Scottrade as financial institution, and SEC registered broker dealer, was trusted by its customers to safeguard their life savings, children's college saving accounts, and retirement accounts. Scottrade had a special duty to exercise reasonable care to protect and secure the PII so as to prevent its collection, theft, or misuse by third parties.

130. Scottrade should have known to take precaution to secure its customers' PII, given its special duty.

131. Scottrade likewise had a duty to exercise reasonable care under the circumstances to prevent any breach of security that would result in the loss, disclosure or compromise of the personal and financial information of Plaintiffs and the Class, given it prior knowledge of security breaches.

132. Scottrade also had a duty to exercise reasonable care under the circumstances to

detect any breach of security that would result in the loss, disclosure or compromise of the personal and financial information of Plaintiffs and the Class.

133. Once a security breach was detected, Scottrade had a duty to exercise reasonable care under the circumstances to notify affected persons in order to minimize potential damage to Plaintiffs and the Class due to the loss, disclosure or compromise of their personal and financial information.

134. Scottrade breached its duty of care by failing to adequately secure and protect Plaintiffs' and the Class members' personal and financial information from theft, collection and misuse by third parties.

135. Scottrade further breached its duty of care by failing to promptly, clearly, accurately, and completely inform Plaintiffs and the Class of the security breach.

136. Plaintiffs' and Class members' PII was transferred, sold, opened, viewed, mined and otherwise released, disclosed, and disseminated without their authorization as the direct and proximate result of Scottrade's failure to design, adopt, implement, control, direct, oversee, manage, monitor and audit its processes, controls, policies, procedures and protocols for complying with the applicable laws and safeguarding and protecting Plaintiffs' and Class Members' PII.

137. The policy of preventing future harm further weighs in favor of finding a special relationship between Scottrade and the Class. Customers count on Scottrade to keep their personal information safe. If companies are not held accountable for failing to take reasonable security measures to protect customers' private and personal information, such as names, social security numbers, and contact information, they will not take the steps that are necessary to protect against future data breaches.

138. It was foreseeable that if Scottrade did not take reasonable security measures, the data of Plaintiffs and members of the Class would be taken.

139. Major financial institutions like Scottrade face a higher threat of security breaches than other smaller businesses due in part to the millions of customers they transact business with.

140. As a direct and proximate result of Scottrade's conduct and breach of its duties, Plaintiffs and the Class members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia,* (i) an imminent, immediate and the continuing increased risk of identity theft and identity fraud, (ii) invasion of privacy, (iii) breach of the confidentiality of their PII, (iv) deprivation of the value of their PII, for which there is a well-established national and international market, (v) failure to receive the full benefit of their bargain as a result of receiving brokerage and financial services that were less valuable than what they paid for; and/or (vi) the financial and/or temporal cost of monitoring their credit, monitoring their financial accounts, and mitigating their damages.

141. Neither Plaintiffs nor other members of the Class contributed to the security breach, nor did they contribute to Scottrade's employment of insufficient security measures to safeguard customers' debit and credit card information.

142. 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.

143. Scottrade's above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach constitute common law negligence, gross negligence, and negligence *per se*.

COUNT IV

Unjust Enrichment / Assumpsit
(On Behalf of Plaintiffs and the National Class, or Alternatively, the Single-State Classes)

144. Plaintiffs re-allege and incorporate by reference Paragraphs 1-106 as if fully set forth herein.

145. By its above-described wrongful actions, inaction, and/or omissions that directly and/or proximately caused the Data Breach – to wit, Scottrade's 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 – Scottrade holds money conferred on it by Plaintiffs and Class Members, *i.e.*, that portion of the fees they paid Scottrade for brokerage and other financial services, allocable to the protection of their PII that Scottrade failed to do. Scottrade has been (and continues to be) unjustly enriched by the funds it should have spent to safeguard and protect Plaintiffs' and Class Members' PII that Scottrade otherwise pocketed that, in equity and good conscience, belongs to Plaintiffs and Class Members, and should be refunded because Scottrade failed to protect their PII.

146. Scottrade also continues to be unjustly enriched by, *inter alia*, (i) the saved cost of implementing the proper PII security measures, policies, procedures, protocols, and software and hardware systems in its computer system and servers, which it did not implement, (ii) the shifted risk and expense of the Data Breach to Plaintiffs and Class Members, and (iii) the return on investment on all above-described amounts.

147. Scottrade, therefore, should be compelled to refund (or disgorge) such wrongfully collected, saved back and/or shifted funds and expenses under the common law equitable doctrine of assumpsit.

COUNT V

Declaratory Relief
(On Behalf of Plaintiffs and the National Class, or Alternatively, the Single-State Classes)

148. Plaintiffs re-allege and incorporate by reference Paragraphs 1-106 as if fully set forth herein.

149. An actual controversy has arisen in the wake of the Data Breach regarding Scottrade's duties to safeguard and protect Plaintiffs' and Class members' confidential and sensitive PII. Scottrade's PII security measures were (and continue to be) woefully inadequate. Scottrade disputes these contentions and contends that its security measures are appropriate.

150. Plaintiffs and Class members continue to suffer damages, other injury or harm as additional identity theft and identity fraud occurs.

151. Therefore, Plaintiffs and Class members request a judicial determination of their rights and duties, and ask the Court to enter a judgment declaring, inter alia, (i) Scottrade 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 Data Breach, (ii) Scottrade breached (and continues to breach) such legal duties by failing to safeguard and protect Plaintiffs' and Class members' confidential and sensitive PII, and (iii) Scottrade's breach of its legal duties directly and proximately caused the Data Breach, and the resulting damages, injury, or harm suffered by Plaintiffs and Class members. A declaration from the court ordering Scottrade to stop its illegal practices is required. Plaintiffs and Class Members will otherwise continue to suffer harm as alleged above.

COUNT VI

Violation of the Missouri Merchandising Practices Act and Substantially Similar Laws of the Consumer Fraud States (On Behalf of Plaintiffs and the Consumer Fraud Multistate Class)

152. Plaintiffs re-allege and incorporate by reference Paragraphs 1-106 as if fully set forth herein.

153. Plaintiffs and the other members of the Class were deceived by Scottrade's failure to properly implement adequate, commercially reasonable security measures to protect their private personal and financial information in the face of Scottrade's repeated representations and assurances to the contrary.

154. Scottrade intended for Plaintiffs and the other members of the Class to rely on its representations and assurances that the information furnished to Scottrade would be protected, secure, and not susceptible to access from unauthorized third parties when Scottrade knew otherwise.

155. Scottrade mishandled Plaintiffs' and the other Class members' personal information in such a manner that it was compromised. Scottrade failed to follow industry best practices concerning data theft or was negligent in preventing such data theft from occurring.

156. Scottrade accordingly engaged in an unlawful unfair and deceptive practice under Mo. Stat. Ann. §407.020.

157. It was foreseeable that Scottrade's willful indifference or negligent course of conduct in handling their customers' personal information would put that information at risk of compromise by data thieves.

158. Scottrade benefited from mishandling customers' personal information because, by not taking preventative measures that would have prevented the data from being compromised, Scottrade saved on the cost of those security measures.

159. Scottrade's fraudulent and deceptive acts and omissions were intended to induce Plaintiffs' and the other Class members' reliance on Scottrade's deception that their personal and financial information was secure and protected.

160. Scottrade violated Mo. Ann. Stat. §407.020 by failing to properly implement adequate, commercially reasonable security measures to protect Plaintiffs' and the other Class members' private personal and financial information, by misrepresenting the security of Plaintiffs' and Class members personal information, by failing to warn them that their information was at risk before and/or after Plaintiffs and Class members opened accounts with Scottrade, and by failing to discover and immediately notify affected customers of the nature and extent of the Data Breach.

161. Scottrade's acts or practice of failing to employ reasonable and appropriate security measures to protect consumers' personal information constitute violations of the Federal Trade Commission Act, 15 U.S.C. §45(a).

162. Scottrade's conduct constitutes unfair acts or practices as defined in that statute because Scottrade caused substantial injury to Plaintiffs and Class members that is not offset by countervailing benefits to consumers or competition and is not reasonably avoidable by consumers.

163. Plaintiffs and the other Class members have suffered injury in fact and actual damages including lost money and property as a result of Scottrade's violations.

164. Plaintiffs' and the other Class members' injuries were proximately caused by Scottrade's fraudulent and deceptive behavior, which was conducted with wanton, willful, and/or outrageous acts and/or reckless disregard for the rights of others, such that an award of punitive damages is appropriate under Mo. Stat. Ann. §407.025.1.

165. By this conduct, Scottrade violated the substantive consumer protection and unfair deceptive trade practices acts or statutes of the Consumer Fraud States, whose laws do not materially differ from that of Missouri, or conflict with each other for purposes of this action.

COUNT VII

Violation of the Missouri Merchandising Practices Act (In the Alternative to Count VI, and on Behalf of Plaintiffs Duqum and Obringer, and the Missouri and Nevada Classes)

166. Plaintiffs re-allege and incorporate by reference Paragraphs 1-106 as if fully set forth herein.

167. Plaintiffs Duqum and Obringer and the other members of the Missouri and Nevada Classes were deceived by Scottrade's failure to properly implement adequate, commercially reasonable security measures to protect their private personal and financial information in the face of Scottrade's repeated representations and assurances to the contrary.

168. Scottrade intended for Plaintiffs Duqum and Obringer and the other members of the Missouri and Nevada Classes to rely on its representations and assurances that reasonable, industry leading steps would be taken to protect and secure the PII from access from unauthorized third parties when Scottrade knew otherwise.

169. Scottrade mishandled Plaintiffs' and the other Class members' PII in such manner that it was compromised. Scottrade failed to follow industry best practices concerning data theft or were negligent in preventing such data theft from occurring.

170. Scottrade accordingly engaged in an unlawful unfair and deceptive practice under Mo. Stat. Ann. §407.020.

171. It was foreseeable that Scottrade's willful indifference or negligent course of conduct in handling their customers' personal information would put that information at risk of compromise by data thieves.

172. Scottrade benefited from mishandling customers' personal information because, by not taking preventative measures that would have prevented the data from being compromised, Scottrade saved on the cost of those security measures.

173. Scottrade's fraudulent and deceptive acts and omissions were intended to induce Plaintiffs' and the other Class members' reliance on Scottrade's deception that their personal and financial information was secure and protected.

174. Scottrade violated Mo. Ann. Stat. §407.020 by failing to properly implement adequate, commercially reasonable security measures to protect Plaintiffs' and the other Class members' private personal and financial information, by misrepresenting the security of Plaintiffs' and Class members PII, by failing to warn them that their information was at risk before and/or after Plaintiffs and Class members opened accounts with Scottrade, and by failing to discover and immediately notify affected customers of the nature and extent of the Data Breach.

175. Scottrade's acts or practice of failing to employ reasonable and appropriate security measures to protect consumers' personal information constitute violations of the Federal Trade Commission Act, 15 U.S.C. §45(a).

176. Scottrade's conduct constitutes unfair acts or practices as defined in that statute because Scottrade caused substantial injury to Plaintiffs and Class members that is not offset by

countervailing benefits to consumers or competition and is not reasonably avoidable by consumers.

177. Plaintiffs and the other Class members have suffered injury in fact and actual damages including lost money and property as a result of Scottrade's violations.

178. Plaintiffs' and the other Class members' injuries were proximately caused by Scottrade's fraudulent and deceptive behavior, which was conducted with wanton, willful, and/or outrageous acts and/or reckless disregard for the rights of others, such that an award of punitive damages is appropriate under Mo. Stat. Ann. §407.025.1.

COUNT VIII

Violations of the California Customer Records Act
California Civil Code §1798.80, *et seq*.
(In the Alternative to Count VI, and on Behalf of Plaintiff Hine and the California Class)

179. Plaintiffs re-allege and incorporate by reference Paragraphs 1-106 as if fully set forth herein.

180. "[T]o ensure that personal information about California residents is protected," the California Legislature enacted the Customer Records Act (the "California CRA"), California Civil Code §1798.81.5, which requires that any business that "owns licenses, or maintains 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."

181. The events alleged herein constituted a "breach of the security system" of Scottrade within the meaning of California Civil Code §1798.82.

182. The information lost, disclosed, or intercepted during the events alleged herein constituted unencrypted "personal information" within the meaning of California Civil Code §§1798.80(e) and 1798.82(h).

183. Scottrade failed to implement and maintain reasonable or appropriate security procedures and practices measures to protect customers' personal and financial information. On information and belief, Scottrade failed to employ industry standard security measures, best practices or safeguards with respect to customers' personal and financial information.

184. Scottrade failed to disclose the breach of security of its system in the most expedient time possible and without unreasonable delay after it knew or reasonably believed that customers' personal information had been compromised.

185. The breach of the personal information of millions of accounts of Scottrade customers constituted a "breach of the security system" of Scottrade pursuant to Civil Code §1798.82(g).

186. By failing to implement reasonable measures to protect its customers' personal data, Scottrade violated Civil Code §1798.81.5.

187. In addition, by failing to promptly notify all affected Scottrade customers that their personal information had been acquired (or was reasonably believed to have been acquired) by unauthorized persons in the data breach, Scottrade violated Civil Code §1798.82 of the same title in a manner that would reach all affected customers.

188. By violating Civil Code §§1798.81.5 and 1798.82, Scottrade "may be enjoined" under Civil Code §1798.84(e).

189. Accordingly, Plaintiff Hine requests that the Court enter an injunction requiring Scottrade to implement and maintain reasonable security procedures to protect customers' data in

compliance with the California Customer Records Act, including, but not limited to: (1) ordering that Scottrade, 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 Scottrade's systems on a periodic basis; (2) ordering that Scottrade engage third party security auditors and internal personnel, consistent with industry standard practices, to run automated security monitoring; (3) ordering that Scottrade audit, test, and train its security personnel regarding any new or modified procedures; (4) ordering that Scottrade, consistent with industry standard practices, conduct regular database scanning and security checks; (5) ordering that Scottrade, 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; and (6) ordering Scottrade to meaningfully educate its customers about the threats they face as a result of the loss of their financial and personal information to third parties, as well as the steps Scottrade customers must take to protect themselves.

190. Plaintiff Hine further requests that the Court require Scottrade to: (1) identify and notify all members of the Class who have not yet been informed of the data breach; and (2) to notify affected customers of any future data breaches by email and text within 24 hours of Scottrade's discovery of a breach or possible breach and by mail within 72 hours.

191. As a result of Scottrade's violation of Civil Code §§1798.81, 1798.81.5, and 1798.82, Plaintiff Hine and California Class members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*, (i) an imminent, immediate and the continuing increased risk of identity theft and identity fraud, (ii) invasion of privacy, (iii) breach of the confidentiality of their PII, (iv) deprivation of the value of their PII,

for which there is a well-established national and international market, (v) failure to receive the full benefit of their bargain as a result of receiving brokerage and financial services that were less valuable than what they paid for; and/or (vi) the financial and/or temporal cost of monitoring their credit, monitoring their financial accounts, and mitigating their damages.

192. Plaintiff Hine, individually and on behalf of the members of the California Class, seeks all remedies available under Civil Code §1798.84, including, but not limited to: (a) damages suffered by members of the California Class; and (b) equitable relief. Plaintiff Hine, individually and on behalf of the members of the California Class, also seeks reasonable attorneys' fees and costs under applicable law.

COUNT IX

Violations of the California Unfair Competition Law
Cal. Bus. & Prof. Code §17200, *et seq.*
(In the Alternative to Count VI, and on Behalf of Plaintiff Hine and the California Class)

193. Plaintiffs re-allege and incorporate by reference Paragraphs 1-106 as if fully set forth herein.

194. 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. By virtue of its above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach, Scottrade engaged in unlawful, unfair and fraudulent practices within the meaning, and in violation of, the UCL.

195. In the course of conducting its business, Scottrade committed "unlawful" business practices by, *inter alia*, knowingly failing to design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures,

protocols, and software and hardware systems to safeguard and protect Plaintiff Hine's and California Class members' PII, and violating the statutory and common law alleged herein in the process, including, *inter alia,* the Federal Trade Commission Act (15 U.S.C. §45), California's Customer Records Act (Cal. Civ. Code §1798.80, *et seq.*), California's Information Practices Act (Cal. Civ. Code §1798.1, *et seq.*), California's UCL, and common law negligence. Plaintiff Hine and California Class members reserve the right to allege other violations of law by Scottrade constituting other unlawful business acts or practices. Scottrade's above-described wrongful actions, inaction, omissions, and want of ordinary care are ongoing and continue to this date.

196. Scottrade also violated the UCL by failing to timely notify Plaintiff Hine and California Class members regarding the unauthorized release and disclosure of their PII.

197. Scottrade's above-described wrongful actions, inaction, omissions, want of ordinary care, misrepresentations, practices, and non-disclosures also constitute "unfair" business acts and practices in violation of the UCL in that Scottrade's wrongful conduct is substantially injurious to consumers, offends public policy, and is immoral, unethical, oppressive, and unscrupulous. California has a well-defined public policy embodied by various states statutes, including the California's Customer Records Act and Information Practices Act to ensure that businesses that maintain customer's personal information implement and maintain reasonable security procedure and practices to protect the personal information from unauthorized access, destruction, use, modification or disclosure. The gravity of Scottrade's wrongful conduct outweighs any alleged benefits attributable to such conduct. There were reasonably available alternatives to further Scottrade's legitimate business interests other than engaging in the above-described wrongful conduct.

198. The UCL also prohibits any "fraudulent business act or practice." Scottrade's above-described claims, nondisclosures and misleading statements were false, misleading and likely to deceive the consuming public in violation of the UCL.

199. As a direct and proximate result of Scottrade's above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach and its violations of the UCL, Plaintiff Hine and California Class members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia,* (i) an imminent, immediate and the continuing increased risk of identity theft and identity fraud, (ii) invasion of privacy, (iii) breach of the confidentiality of their PII, (iv) deprivation of the value of their PII, for which there is a well-established national and international market, (v) failure to receive the full benefit of their bargain as a result of receiving brokerage and financial services that were less valuable than what they paid for; and/or (vi) the financial and/or temporal cost of monitoring their credit, monitoring their financial accounts, and mitigating their damages.

200. Unless restrained and enjoined, Scottrade will continue to engage in the above-described wrongful conduct and more data breaches will occur. Plaintiff Hine, therefore, on behalf of himself, California Class members, and the general public, also seeks restitution and an injunction prohibiting Scottrade from continuing such wrongful conduct, and requiring Scottrade to modify its corporate culture and design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures protocols, and software and hardware systems to safeguard and protect the PII entrusted to it, as well as all other relief the Court deems appropriate, consistent with Cal. Bus. & Prof. Code §17203.

COUNT X

Violations of the Florida Deceptive and Unfair Trade Practices Act
Fla. Stat. §501.201, *et seq.*
(In the Alternative to Count VI,
and on Behalf of Plaintiff Kuhns and the Florida Class)

201. Plaintiffs re-allege and incorporate by reference Paragraphs 1-106 as if fully set forth herein.

202. The Florida Deceptive and Unfair Trade Practices Act ("FDUTPA"), Fla. Stat. §501.201, *et seq.* makes unlawful any "[u]nfair methods of competition, unconscionable acts or practices, and unfair or deceptive acts or practices in the conduct of any trade or commerce."

203. Scottrade's conduct, as alleged herein, constitutes unconscionable, unfair, and deceptive acts or practices in violation of FDUTPA.

204. Scottrade's unconscionable, unfair, and deceptive acts and omissions took place in the conduct of trade or commerce. Under FDUTPA, "trade or commerce" is defined to include, inter alia, "providing [or] offering . . . any service." Fla. Stat. §501.203(8).

205. Scottrade intended for Plaintiff and the Florida Class to rely on these unconscionable, unfair, and deceptive acts and omissions when Plaintiff and the Class opened accounts with Scottrade.

206. Plaintiff and the Florida Class have suffered injuries in fact and actual damages resulting from Scottrade's violations of FDUTPA. These injuries are of the type FDUTPA was designed to prevent, and are the direct and proximate result of Scottrade's unlawful conduct.

207. Accordingly, Plaintiff and the Florida Class are entitled to a declaratory judgment that Scottrade's acts or practices, as alleged herein, violate FDUTPA, as well as an

injunction prohibiting Scottrade from engaging in such acts or practices in the future and any and all damages, fees, and costs permitted by law.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and all persons and consumers similarly situated, pray for judgment as follows:

A. An Order certifying the proposed Classes defined herein, designating Plaintiffs as representative of said Classes, and appointing the undersigned counsel as Class Counsel;

B. For restitution of all amounts obtained by Scottrade as a result of its wrongful conduct in an amount according to proof at trial, plus pre-judgment and post-judgment interest thereon;

C. For all recoverable compensatory, consequential, actual, and/or statutory damages in the maximum amount permitted by law;

D. For punitive and exemplary damages;

E. For other equitable relief;

F. For such injunctive relief, declaratory relief, orders, or judgment as necessary or appropriate to prevent these acts and practices;

G. For payment of attorneys' fees and costs of suit as allowable by law; and

H. For all such other and further relief as the Court deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand a jury trial on all issues so triable, as provided by Rule 38 of the Federal Rules of Civil Procedure.

Dated: February 19, 2016

s/ Joseph J. Siprut
JOSEPH J. SIPRUT

SIPRUT PC
JOSEPH J. SIPRUT
JOHN S. MARRESE
17 North State Street, Suite 1600
Chicago, IL 60602
Tel: 312/236-0000
312/878-1342 (fax)
jsiprut@siprut.com
jmarrese@siprut.com

Proposed Class Counsel

Dated: February 19, 2016

s/ Timothy G. Blood
TIMOTHY G. BLOOD

BLOOD HURST & O'REARDON, LLP
TIMOTHY G. BLOOD (*pro hac vice*)
THOMAS J. O'REARDON II (247952CA)
PAULA R. BROWN (254142CA)
701 B Street, Suite 1700
San Diego, CA 92101
Tel: 619/338-1100
619/338-1101 (fax)
tblood@bholaw.com
toreardon@bholaw.com
pbrown@bholaw.com

Proposed Class Counsel

THE SIMON LAW FIRM, P.C.
ANTHONY G. SIMON
JOHN M. SIMON
800 Market Street, Suite 1700
St. Louis, MO 63101
Tel: 314/241-2929
314/241-2029 (fax)
asimon@simonlawpc.com
jsimon@simonlawpc.com

LITE DE PALMA GREENBERG
KATRINA CARROLL
KYLE A. SHAMBERG
211 W. Wacker Drive, Suite 500
Chicago, IL 60606
Tel: 312/750-1265
312/212-5919 (fax)
kcarroll@litedepalma.com
kshamberg@litedepalma.com

COHELAN KHOURY & SINGER
TIMOTHY D. COHELAN (60827CA)
J. JASON. HILL (*pro hac vice*)
605 C Street, Suite 200
San Diego, CA 92101
Tel: 619/595-3001
619/595-3000 (fax)
tcohelan@ckslawfirm.com
jhill@ckslaw.com

SPRETER LAW FIRM, APC
GEOFF SPRETER (257707CA)
402 W. Broadway, Suite 860
San Diego, CA 92101
Tel: 619/865-7986

geoff@spreterlaw.com

Proposed Executive Committee Members

E. ELLIOT ADLER (229030CA)
402 W. Broadway, Suite 860
San Diego, CA 2101
Tel: 619/531-8700
619/342-9600 (fax
elliotadler@gmail.com

DOGALI LAW GROUP, P.A.
ANTHONY ANDERSON BENTON DOGALI
GEOFFREY E. PARMER
101 E. Kennedy Blvd., Suite 1100
Tampa, FL 33602-5146
Tel: 813/289-0700
813/289-9435 (fax)
gparmer@dogalilaw.com

LOCKRIDGE AND GRINDAL
KATE M. BAXTER-KAUF
KAREN HANSON RIEBEL
100 Washington Avenue S., Suite 2200
Minneapolis, MN 55401
Tel: 612/339-6900
612/339-0981 (fax)
kmbaxter-kauf@locklaw.com
kriebekh@locklaw.com

Additional Counsel for Plaintiffs

CERTIFICATE OF SERVICE

I hereby certify that service of the foregoing has been made through the Court's CM/ECF system on all counsel of record. Executed on February 19, 2016, at Chicago, Illinois.

s/ Joseph J. Siprut