Timothy D. Cohelan, Esq. (SBN #60827)
tcohelan@ckslaw.com
J. Jason Hill, Esq. (SBN #179630)
jhill@ckslaw.com
COHELAN KHOURY & SINGER
605 C Street, Suite 200
San Diego, California 92101
Telephone: (619) 595-3001
Fax: (619) 595-3000

E. Elliot Adler, Esq. (SBN #229030)
eadler@theadlerfirm.com
ADLER LAW GROUP, APLC
402 West Broadway, Suite 860
San Diego, California 92101
Telephone:(619) 531-8700
Fax: (619) 342-9600

Geoffrey J. Spreter, Esq. (SBN #257707)
geoff@spreterlaw.com
SPRETER LAW FIRM, APC
402 W. Broadway, Suite 860
San Diego, CA 92101
Tel: (619) 865-7986

Attorneys for Plaintiff and the Proposed Class

UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF SOUTHERN CALIFORNIA

STEPHEN HINE, individually and on behalf of all others similarly situated,

Plaintiff,

v.

Scottrade, Inc, a Missouri Corporation.

Defendants.

Case No. **'15CV2213 W JMA**

CLASS ACTION COMPLAINT

1. **VIOLATIONS OF CALIFORNIA CONSUMER'S RECORDS ACT;**
2. **NEGLIGENCE;**
3. **CONCEALMENT**
4. **BREACH OF FIDUCIARY DUTY;**
5. **VIOLATIONS OF CALIFORNIA BUS. & PROF. CODE §17200 et seq.**

JURY TRIAL DEMANDED

Plaintiff, Stephen Hine, an individual ("Plaintiff"), individually and on behalf of all others similarly situated, bring this action against Defendant, Scottrade, Inc. ("Scottrade"), for damages, equitable relief, demand a trial by jury.

INTRODUCTION

1. Starting in late 2013, and continuing for several months and into early 2014, the confidential contact information, including social security numbers, tax identification numbers, employer contact information, personal email addresses, and other sensitive data, of about 4.6 million investors and customers of Defendant Scottrade, was accessed in a massive data breach that was the result of an external criminal act.

2. On October 2, 2015, news media outlets began reporting on the potential data breach affecting Scottrade's millions of customers. The customers had, among other things, their brokerage accounts, retirement accounts, children's college saving accounts, personal bank accounts with Scottrade.

3. Scottrade confirmed the data breach the same day, and said that the company first learned of the breach after governmental officials informed them that they had been investigating cybersecurity crimes, involving the theft of information from Scottrade and other financial services companies.[1]

4. In addition, Scottrade stated that it was beginning to notify investors who were potentially affected by the breach, some of whom were sent emails. But Scottrade is

[1] http://krebsonsecurity.com/2015/07/experian-hit-with-class-action-over-id-theft-service/

not sure and "may never know" the exact number of individuals who names and addresses were affected by the breach.[2]

5. Almost instantly after Scottrade's statements, news outlets began to speculate that the security breach involving Scottrade may somehow be tied to the security breaches of several banks and other financial institutions, including J.P. Morgan Chase, which occurred in 2014.

6. The J.P Morgan Chase breach resulted in the theft of nearly 76 million household's contact information. According to several online blogposts and newspaper articles, the J.P Morgan Chase breach was easily preventable had J.P. Morgan Chase applied a simple security fix.

7. In fact, according to a New York Times article from December 22, 2014:

> "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 JP Morgan Chase was. To date, only two other financial institutions have suffered some kind of intrusion, but those breaches were said to be relatively minor by people briefed on the attacks." [3]

8. In July 2015, five (5) individuals were formally charged for the J.P. Morgan Chase breach by federal prosecutors.[4] It was alleged that they obtained the information "to further stock manipulation schemes involving spam emails to pump up the price of otherwise worthless penny stocks." [5]

---

[2] http://www.wired.com/2015/10/scottrade-alerts-4-6-million-brokerage-customers-breach/
[3] http://dealbook.nytimes.com/2014/12/22/entry-point-of-jpmorgan-data-breach-is-identified/
[4] http://fortune.com/2015/10/02/scottrade-data-breach/
[5] Id.

9. As discussed further below, Scottrade was negligent in failing to exercise reasonable security precautions, failing to comply with industry standards for storing confidential and private personal information. Moreover, when Scottrade notified the affected customers of the breach via email their notification was woefully inadequate and vague, given the threat that currently exists concerning the potential use of their private information in stock scams, other financial frauds, and its sale on the black market.

10. Scottrade's actions and/or omissions occurred despite prior warnings, including prior incursions of their network by third parties, who conducted fraudulent stock trades using Scottrade's customer's accounts, and even fines from government agencies concerning its system's security procedures and oversight.

11. Had Scottrade taken necessary precautions to protect its customers' personal and private information, it would have prevented the breach that has now affected approximately 4,600,000 customers altogether -- or at a minimum detected it much sooner, reducing the harm to its customers who entrusted Scottrade with their confidential and highly sensitive personal information.

12. Plaintiff Stephen Hine is a Scottrade investor who brings this proposed class action lawsuit on behalf of Scottrade customers nationwide, and on behalf of a California subclass, alleging that Scottrade failed to adequately safeguard its customers' private and personal information in compliance with applicable statutes and industry standard business practices. Plaintiff seeks injunctive relief, requiring

Scottrade to obtain appropriate security as to comply with regulations designed to prevent these types of breaches, damages, restitution, and other remedies, and to provide notice sufficient to address the scope of the breach and using a method designed to reach all customers affected by the breach.

VENUE AND JURSDICTION

13. This Court has personal and subject matter jurisdiction over all causes of action asserted herein.

14. This Court has jurisdiction over this action pursuant to the Class Action Fairness Act of 2005 28 U.S.C. §1332(d)(2). In the aggregate, the claims of Plaintiff and other members of the putative Classes exceed $5,000,000 exclusive of interest and costs. In addition, at least one class member is a citizen of a different state than defendant Scottrade, and there are more than 1,000 putative class members.

15. This Court has personal jurisdiction over Scottrade because Scottrade is authorized to conduct business in California, and does in fact conduct business in California by operating retail stores within the State. Scottrade therefore has sufficient minimum contacts with the state to render exercise of jurisdiction by this Court in compliance with traditional notions of fair play and substantial justice.

16. Venue is proper in this judicial district pursuant to 28 U.S.C. § 1391 because Scottrade regularly conducts business in this district, unlawful acts or omissions are alleged to have occurred in this district, and Scottrade is subject to personal jurisdiction in this district.

17. Plaintiff Stephen Hine is an individual and a California resident. Believing that Scottrade would safeguard his personal information, Plaintiff provided his confidential and highly sensitive personal and private information to Scottrade to open a brokerage account.

18. Defendant Scottrade is a Missouri corporation with its headquarters and principal place of business in Missouri.

19. 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.[6] 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.

20. 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."

21. 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.[7] Identity thieves use stolen personal

[6] *See* http:///www.gao.gov/new.items/d07737.pdf.
[7] *See* FTC Identity Theft Website: www.ftc.gov/bcp/edu/microsites/idtheft/consumers/about-identity-theft.html.

information such as SSNs for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[8]

22. 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.

23. 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. [9]

24. 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

---

[8] 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*.

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

> attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm."

25. Sensitive information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for a number of years.[10] As a result of recent large-scale data breaches, identity thieves and cyber criminals have openly posted stolen credit card numbers, SSNs, and other Sensitive Information directly on various Internet websites making the information publicly available. In one study, researchers found hundreds of websites displaying stolen 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."[11]

26. It's within this context that Plaintiff and the nearly 4.6 million customer of Scottrade who relied on Scottrade's Privacy and Security policies

---

[10] Companies, in fact, also recognize 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. Risk Assessment Tool, Norton 2010, www.everyclickmatters.com/victim/assessment-tool.html. *See also* 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).

[11] http://www.stopthehacker.com/2010/03/03/the-underground-credit-card-blackmarket/

must now live with the knowledge that their personal information is now forever out in cyberspace and available for sale on the black-market.

SCOTTRADE FAILED TO HONOR ITS PRIVACY POLICY AND AGREEMENTS TO KEEP SENSITIVE PERSONAL INFORMATION CONFIDENTIAL

27. Scottrade is a privately owned discount retail brokerage firm headquartered in Town and Country, Missouri and does business in all 50 States. Scottrade's currently has 503 branch offices around the United States and has over 3,720 employees. [12]

28. Scottrade became popular in the late 1990's during the dot.com bubble based upon its low $7.00 online trading platform.

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

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

31. In order to sign up for one of the Scottrade investment accounts, customers must provide certain personal and confidential information to Scottrade during the sign up process for a new account.[13] Among other things Scottrade,

[12] https://en.wikipedia.org/wiki/Scottrade

[13] https://www.scottrade.com/documents/alt/PrivacyStatement.pdf

collects names, addresses, phone numbers, social security numbers, work history and other personal identifying information.

32. According to Scottrade online privacy policy, Scottrade collects personal information from customers during the below transactions:

> "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."[14]

33. Scottrade makes several representations during the sign up process, including that while clients are doing business with Scottrade, the company will respect the client's privacy and keep sensitive information confidential.

34. For example, on its website, and with respect to Scottrade's privacy statement, Scottrade make the following statement:

> **"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.
>
> 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." [15]
>
> …
>
> **"Scottrade Privacy Statement**

[14] Id.

[15] https://www.scottrade.com/online-brokerage/secure-trading.html

> To 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." [16]

35. At all times relevant, Scottrade had the above privacy policy in effect and made such representations to Plaintiff and the Class. Scottrade made the representation that its takes security very seriously and assured customers that it would keep all personal and confidential information secure using various physical, electronic and procedural safeguards.

36. Plaintiff 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 a customer's decision to invest with Scottrade.

THE 2013 THROUGH 2014 SCOTTRADE DATA BREACH

37. 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.[17] Ironically, the breach occurred on the 2nd day of "Cyber Security Awareness Month."

[16] https://www.scottrade.com/documents/alt/PrivacyStatement.pdf

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

38. 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. [18]

39. 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."

40. 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, Scottrade's spokesperson Ms. Leordeanu said the company couldn't comment on the incident much more in the information included in its website notice about the attack.[19] She did, however, state

[18] Id.
[19] Id.

that "Scottrade learned about the date of theft from the FBI, and the company is working with agents from FBI field offices and Atlanta and New York."[20]

41. Mr. Krebs surmises 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.

42. Numerous online news sites are reporting or indicating 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.[21]

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

44. The troubling fact about the J.P. Morgan breach is that according to a New York Times article the attack itself *could have been completely preventable*. 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.
>
> …

[20] Id.

[21] http://fortune.com/2015/10/02/scottrade-data-breach/

> 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.
>
> 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." [22]

45. 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 regrading network security, as well maintain proper supervisory mechanisms involving wire transfers: [23]

> "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."

---

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

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

> 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."

46. According to an article on MarketWatch.com, dated October 9, 2014 from www.marketwatch.com from brokerage firms were hacked during the period of 2014.[24] "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."

47. The online brokerage firms involved in the incident promptly reimbursed their customers who were affected by the hack and breach. In response, to the privacy breaches of the brokerage firms, Scottrade's spokeswoman said the firm couldn't comment on this case specifically.[25]

SCOTTRADE'S DATA BREACH NOTIFICATION EMAIL AND OFFERED "REMEDY" ARE INADEQUATE AND CREATE A BURDEN ON THE AFFECTED CUSTOMERS

48. On October 2, 2015 Scottrade began formally notifying Plaintiff and Class Members about the data breach via email, confirming that the security of their personal and private information- that Scottrade received from them during the

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

course of their investment relationship – including, but not limited to: (i) names, (ii) addresses, (iii) Social Security numbers, (iv) employers' names; (v) tax identification numbers.

49. Many affected customers will not receive the emails, However, because the affected customers may have changed email addresses, or use alternative email addresses for personal and financial matters. Scottrade could have 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 emails.

50. The data breach emails are materially misleading and do not fully disclose the scope of the threat to Scottrade's customers.

51. Scottrade advises the recipients of the emails that their personal information "*may* have been compromised" in 2013 through 2014. Scottrade also states that it is not aware which specific personal customer information was actually taken during the 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 email). It is highly unlikely that the hackers, having access to the above information, would only take the affected customer's name and email address.

52. The data breach email also fails 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, how the breach occurred, and 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."

53. The data breach email also squarely places the burden on Plaintiff and the Class, rather than Scottrade, to protect themselves and mitigate their data breach damages – customers are instructed to review their account statements, monitoring 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."

54. The data breach email also states that Scottrade will provide one year of free credit monitoring and identity theft insurance to all affected persons. The offered "credit monitoring," however, is inadequate and requires the 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 athttps://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.

55. Unfortunately, many of Scottrade's other mitigation suggestions require Plaintiff and Class to incur additional out-of-pocket expenses to protect themselves from the 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

56. As a general rule in California, the fee to place (and remove) a "security freeze" on one's credit report, as suggested by the Data Breach emails, is $10 each

time it is placed at each of the three credit reporting agencies (Experian, Equifax, and TransUnion).

57. Monitoring one's credit reports, another option suggested by the Data Breach email, 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.

58. Affected customers are also instructed place fraud alerts, which also costs the Scottrade customers additional time and money:

> 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.

59. At all times alleged in this complaint, 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 financial information and other sensitive information.

60. As customers of Scottrade, Plaintiff Hine and the Class provided Scottrade with their accurate personal information, as required under their service agreements with Scottrade and relied on Scottrade representations that it would keep it would securely store and keep their personal information private.

61. Despite knowledge of the susceptibility of Scottrade's online network to intrusion from outside 3rd parties, including the existence of prior intrusions, and

lack of internal supervisory mechanisms, Scottrade continued to make the representation that client's personal and private information was safe and secure with Scottrade. Plaintiff and the class relied on Scottrade's representations concerning security and privacy and continued to do business with Scottrade.

62. Scottrade's wrongful actions, inaction, omissions, and want of ordinary care in failing to completely and accurately notify Plaintiff and the Class, using methods and means to reach all affected class member, such as text message, pre-recorded phone calls, about the data breach and corresponding unauthorized release and disclosure of their personal information was arbitrary, capricious and in derogation of Scottrade's fiduciary duties owed to Plaintiff and the Class.

CLASS ALLEGATIONS

63. Pursuant to Rule 23(b) of the Federal Rules of Civil Procedure, Plaintiff brings this class action lawsuit on behalf of himself and all other members of the Class (the **"Class"**) defined as follows:

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

64. In addition to, and in the alternative, Plaintiff seeks certification of a National and California Subclass (the "California Class" or "California Subclass") defined as follows:

> All persons and entities in California whose personal or financial

information was compromised as a result of the data breach first disclosed by Scottrade on October 2, 2015.

65. Excluded from the Classes are: (1) Defendants 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.

66. **Numerosity.** Scottrade is one the largest online discount brokerage firms in the United States with approximately 503 offices. Scottrade has admitted the personal information, including names, mailing addresses, phone numbers, and email addresses of approximately 4,600,000 million customers was also stolen during the security breach. Plaintiff therefore believes that the Class is so numerous that joinder of all members is impractical.

67. **Typicality.** Plaintiff's claims are typical of the claims of the Class. Plaintiff and the Class members were injured by the same wrongful acts, practices, and omissions committed by Scottrade, as described herein. Plaintiff's claims therefore arise from the same practices or course of conduct that give rise to the claims of all Class members.

68. **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 interception by investing with Scottrade;

H. Whether Scottrade's conduct violated Cal. Civ. Code § 1798.80 et seq.;

I. Whether Scottrade intentionally failed to disclose material information regarding its security measures, the risk of data interception, and/or the ongoing security breach;

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

K. Whether Scottrade's conduct violated California's Unfair Competition Law (Cal. Bus. & Prof. Code § 17200 et seq.);

L. Whether Scottrade's conduct was negligent;

M. Whether Plaintiff and the Class members are entitled to restitution, disgorgement, and/or other equitable relief; and

N. Whether Plaintiff and the Class members are entitled to recover actual damages, statutory damages, and/or punitive damages.

69. **Adequacy.** Plaintiff will fairly and adequately protect the interests of the Class members. Plaintiff is an adequate representative of the Class in that he has no interests which are adverse to or conflict with those of the Class members Plaintiff seeks to represent. Plaintiff has retained counsel with substantial experience and success in the prosecution of complex consumer protection class actions of this nature.

70. **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 a contrast, a class action presents fewer management difficulties and provides the benefits of single adjudication and comprehension supervision by a single court.

FIRST CLAIM FOR RELIEF
Violations of California Civil Code §1798.80, et seq.
(On Behalf of Plaintiff and the Classes)

71. Plaintiff hereby re-alleges and incorporates by reference all paragraphs set forth above.

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

73. 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).

74. 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.

75. Scottrade failed to disclose the breach of security of its system, using means and methods to reach all affected customers, in the most expedient time possible and without unreasonable delay after it knew or reasonably believed that customers' personal information had been compromised.

76. 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 section 1798.82(g).

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

78. 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 section 1798.82 of the same title in a manner that would reach all affected customers.

79. By violating Civil Code sections 1798.81.5 and 1798.82, Scottrade "may be enjoined" under Civil Code section 1798.84(e).

80. Accordingly, Plaintiff request 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.

81. Plaintiff further request 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, text, and pre-recorded phone call within 24 hours of Scottrade's discovery of a breach or possible breach and by mail within 72 hours.

82. As a result of Scottrade's violation of Civil Code sections 1798.81, 1798.81.5, and 1798.82, Plaintiff and members of the Class have and will incur economic damages relating to time and money spent remedying the breach, expenses for bank fees associated with the breach, late fees from automated billing services associated with the breach, as well as the costs of credit monitoring and purchasing credit reports.

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

SECOND CLAIM FOR RELIEF
Negligence
(On Behalf of Plaintiff and the Classes)

84. Plaintiff re-alleges and incorporates by reference all paragraphs set forth above.

85. During the course of conducting its business, Scottrade collected customers' personal and financial information, including social security numbers, tax identification numbers, home addresses, email addresses, of Plaintiff and the Class.

86. 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 (see paragraph 44), public reprimands by federal agencies concerning lack of system oversight and violations of federal statutes governing security, and failure to remedy said prior violations, prior security alerts, and the potential fraudulent and criminal uses of the information if acquired, among other things.

87. In addition, Scottrade had notice of a possible security breach due to the prior targeting of other large retailers and financial institutions, including

itself, which has had several issues with online security and breaches, by third parties seeking such information.

88. 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 personal and financial information of Plaintiff and the Class so as to prevent its collection, theft, or misuse by third parties.

89. Scottrade should have known to take precaution to secure its customers' data, given its special duty, especially in light of the recent data breaches affecting numerous retailers and financial institutions, as well as from prior direct breaches of its secured networks.

90. 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 Plaintiff and the Class, given it prior knowledge of security breaches.

91. 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 Plaintiff and the Class.

92. 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 Plaintiff and the Class due to the loss, disclosure or compromise of their personal and financial information.

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

94. Scottrade further breached its duty of care by failing to promptly, clearly, accurately, and completely inform Plaintiff and the Class of the security breach using all means and methods of notification likely to reach the affected customers, such as text message and pre-recorded phone calls.

95. 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 data safe. If companies, like Scottrade, 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.

- It was foreseeable that if Scottrade did not take reasonable security measures, the data of Plaintiff and members of the Class would be stolen.
- 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.
- Scottrade was the target of prior incursions and had notice of the potential of future breaches.

96. As a direct and proximate result of Scottrade's conduct and breach of its duties, Plaintiff and the Class members have suffered injury in fact and damages.

97. Neither Plaintiff 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.

98. Plaintiff 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.

THIRD CLAIM FOR RELIEF
Concealment
(On Behalf of Plaintiff and the Classes)

99. Plaintiff re-alleges and incorporates by reference all paragraphs set forth above.

100. Plaintiff is informed and believes that, on a date presently unknown to Plaintiff but on or before October 2, 2015, Scottrade became aware of an ongoing breach of security of its online trading system resulting in the loss, disclosure or compromise of customers' personal and financial information, including that of Plaintiff and the Class.

101. Plaintiff is further informed and believes that, notwithstanding its knowledge of an ongoing breach of security of its online trading system, Scottrade intentionally failed to inform Plaintiff and the Class that investing with Scottrade

could result in the acquisition of their personal and financial information by third parties.

102. Prior to news of the breach breaking on October 2, 2015, Plaintiff and the Class did not know, and could not have known, of the breach of security of Scottrade's online trading system.

103. Plaintiff is informed and believes that Scottrade intended to deceive Plaintiff and the Class by failing to inform Plaintiff and the Class that use of Scottrade online trading platform would result in the acquisition of their personal and financial information by third parties.

104. Plaintiff and the Class further reasonably relied on such deception in that they refrained from canceling their investment accounts with Scottrade, thereby resulting in further and greater risk of incurring fraudulent and unauthorized charges on their accounts.

105. Plaintiff is also informed and believes that, on a date presently unknown to Plaintiff but prior to October 2, 2015, Scottrade became aware that its online trading system was not reasonably secure and/or that it did not have reasonable and best practices, safeguards and data security in place to protect customers' personal and financial information. Scottrade intentionally failed to disclose or actively concealed this material fact from Plaintiff and the Class.

106. Scottrade was under a duty to Plaintiff and the Class to disclose that its online network was not reasonably secure and that it did not have reasonable and

best practices, safeguards and data security in place to protect customers' personal and financial information because: (1) Scottrade was in a superior position to know the true nature of its security system and data security practices; (2) Scottrade had exclusive knowledge that its online trading system was not reasonably secure and/or that it did not have reasonable and best practices, safeguards, and data security in place to protect customers' personal and financial information, neither of which was known to Plaintiff and the Class at the time of their investing with Scottrade; (3) Scottrade actively concealed from Plaintiff and the Class that its online trading system was not reasonably secure and/or that it did not have reasonable and best practices, safeguards, and data security in place to protect customers' personal and financial information.

107. Plaintiff is further informed and believes that Scottrade intended to deceive Plaintiff and the Class by failing to inform Plaintiff and the Class that the online trading system was not reasonably secure and/or that Scottrade did not have reasonable and best practices, safeguards and data security in place to protect customers' personal and financial information.

108. Plaintiff and the Class reasonably relied on Scottrade's deception and omissions in that they continued to maintain their investment accounts with Scottrade, shared personal information with Scottrade. Plaintiff and the Class would have refrained from making such investments, paying commissions on trades using the Scottrade online trading network in question, had they known of that there was

a security breach, that Scottrade's online system was not reasonably secure, and/or that Scottrade did not have reasonable and best practices, safeguards and data security in place to protect customers' personal and financial information.

109. As a result of Scottrade's conduct, Plaintiff and the Class members have suffered damages and been harmed by, among other things: (1) the interception, loss, and disclosure of their personal and financial information; (2) paying commissions and fees to Scottrade that they otherwise would not have made or would have paid less for had they known their personal information was at risk of disclosure.

110. In addition, Plaintiff and the Class will suffer harm through the expenditure of time and resources in connection with: (1) discovering and assessing fraudulent or unauthorized charges; (2) contesting fraudulent or unauthorized charges; (3) adjusting automatic or other billing instructions; (4) credit monitoring and identity theft prevention; Scottrade's conduct as alleged herein constitutes oppression, fraud, and/or malice such that Scottrade is liable for punitive damages.

FOURTH CLAIM FOR RELIEF
Breach of Fiduciary Duty
(On Behalf of Plaintiff and the Classes)

111. Plaintiff repeat and re-allege all previous allegations as if fully set forth herein.

112. As guardians of Plaintiff' and the members of the Classes' personal and private information, Scottrade owed a fiduciary duty to Plaintiff and the Classes to: (1) protect their personal information; (2) timely notify them of a data breach in

manner likely to reach them; and (3) maintain complete and accurate records of what type and where its members' information is stored.

113. Scottrade breached its fiduciary duty to Plaintiff and the Classes by:

a. Failing to properly protect and monitor private information containing Plaintiff and the Class' Personal Sensitive Information;

b. Failing to timely notify and/or warn Plaintiff and the Class of the data breach using all means and methods directed to reach all affected customers;

114. As a result of Scottrade's conduct, Plaintiff and Class members suffer and will continue to suffer damages including, but not limited to, expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; missed wages; expenses and/or time spent initiating fraud alerts; and, the diminished value of the Scottrade services they received. Plaintiff and members of the Classes have suffered and will continue to suffer other forms of injury and/or harm including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

FOURTH CLAIM FOR RELIEF
Violation of California's Unfair Competition Law ("UCL")
(Cal. Bus. & Prof. Code § 17200, et seq.)
(On Behalf of Plaintiff and the Classes)

115. Plaintiff incorporates and re-alleges all other paragraphs in this complaint as if fully set forth herein.

116. Beginning at an exact date unknown to Plaintiff but at least since sometime in or around October 2, 2015, Scottrade has committed and continues to commit acts of unfair competition, as defined by California's Unfair Competition Law ("UCL"), Cal. Bus. & Prof. Code § 17200, et seq.

117. As specifically alleged herein, Scottrade's acts, practices, omissions, and nondisclosures, violate Cal. Civ. Code §§ 1572, 1573, 1709, 1711, 1798.80 et seq., and the common law. Consequently, Scottrade's acts, practices, omissions, and nondisclosures, as alleged herein, constitute unlawful acts and practices within the meaning of Cal. Bus. & Prof. Code § 17200.

118. Scottrade's acts, practices, omissions, and nondisclosures, as alleged herein, threaten a continued violation of Cal. Civ. Code §§ 1709, 1711, 1798.80 et seq., and the common law, violate the policy and spirit of such laws, and otherwise significantly harm consumers.

119. Furthermore, Scottrade's acts, practices, omissions, and nondisclosures are immoral, unethical, oppressive, unscrupulous, and substantially injurious to consumers. The harm to Plaintiff, the Class, and members of the general public substantially outweighs any benefits of Scottrade's conduct. Furthermore, there were reasonably available alternatives to further Scottrade's legitimate business interests, including using best practices to protect the personal and financial information other than Scottrade's wrongful conduct described herein. Consequently, Scottrade's acts, practices, omissions, and nondisclosures constitute

"unfair" business acts and practices within the meaning of Cal. Bus. & Prof. Code § 17200.

120. Scottrade's acts, practices, omissions, and nondisclosures, as alleged herein, are likely to deceive, and did deceive, Plaintiff, the Class, and members of the general public, and consequently constitute "fraudulent" acts and practices within the meaning of Cal. Bus. & Prof. Code § 17200. Scottrade's conduct was likely to deceive reasonable consumers.

121. Scottrade violated the UCL by accepting and storing personal and financial information of Plaintiff and the Class and then failing to take reasonable steps to protect it. In violation of industry standards, best practices, and reasonable consumer expectations, Scottrade failed to safeguard personal and financial information and failed to tell consumers that it did not have reasonable and best practices, safeguards and data security in place to protect their personal and financial information.

122. As a result of Scottrade's conduct, Plaintiff and the Class members have suffered damages and been harmed by, among other things: (1) the interception, loss, and disclosure of their personal and financial information; making purchases from Scottrade that they otherwise would not have made or would have paid less for had they known their personal information was at risk of disclosure. In addition, Plaintiff and the Class have also suffered harm through the expenditure of time and resources in connection with: (1) discovering and assessing fraudulent or unauthorized

charges; (2) contesting fraudulent or unauthorized charges; (3) adjusting automatic or other billing instructions; (4) credit monitoring and identity theft prevention.

123. Plaintiff and the Class seek injunctive relief, restitution and/or disgorgement, and any further relief that the court deems proper. In addition, Plaintiff seeks reasonable attorneys' fees and prays for the relief set forth below.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and all persons and consumers similarly situated, prays for judgment as follows:

a. An Order certifying the proposed Class defined herein, designating Plaintiff as representative of said Class, 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 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

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

Date: October 2, 2015

Respectfully submitted,

/s/ J. Jason Hill
COHELAN KHOURY & SINGER
605 C Street, Suite 200
San Diego, California 92101
Telephone: (619) 595-3001/Fax: (619) 595-3000
JHill@ckslaw.com

/s/ E. Elliot Adler
ADLER LAW GROUP, APLC
402 West Broadway, Suite 860
San Diego, California 92101
Telephone: (619) 531-8700/Fax: (619) 342-9600
EAdler@TheAdlerFirm.com

/s/ Geoffrey J. Spreter
SPRETER LAW FIRM, APC
402 W. Broadway, Suite 860
San Diego, CA 92101
Tel: (619) 865-7986/Fax: (619) 342-9600
Geoff@spreterlaw.com