MARK A. CHAVEZ (SBN 90858)
CHAVEZ & GERTLER, LLP
42 Miller Ave.
Mill Valley, CA 94941
Telephone: (415) 381-5599

GREGORY A. BECK (Admitted Pro Hac Vice)
PUBLIC CITIZEN LITIGATION GROUP
1600 20th St. NW
Washington, DC 20009
Telephone: (202) 588-1000

Attorneys for Plaintiff Matthew Elvey

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

In re TD AMERITRADE ACCOUNTHOLDER LITIGATION	Case No. C 07-2852 VRW CLASS ACTION **PLAINTIFF MATTHEW ELVEY'S OBJECTIONS TO CLASS ACTION SETTLEMENT**

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

CASES (CONT'D.)

STATUTES AND RULES

OTHER AUTHORITIES

INTRODUCTION

This is a proposed class action against TD Ameritrade ("Ameritrade") over the consequences of one of the largest security breaches ever recorded. The security breach allowed outside hackers access to sensitive client data on the company's servers, including social security numbers, birth dates, and account numbers. Def.'s Resp. to June 13 Order ("Def.'s Resp."), Exh. 1 at 1. This security breach was not an isolated loss of data; Ameritrade's clients had complained for at least twenty-three months that their private account data was being stolen. Sweet Decl. ¶ 2; Winzig Decl. ¶ 2. Despite the mounting evidence of a serious security breach, Ameritrade took no action to notify its clients of the problem or warn them that they may be at risk of identity theft. Only after plaintiffs asked the Court to order Ameritrade to disclose the breach did the company finally admit that "unauthorized code" on its systems had allowed outsiders to take "certain information" from its client database. Def.'s Resp., Exh. 1 at 3.

The proposed settlement would release the rights of the class to seek relief against Ameritrade for the breach without providing them with any monetary or injunctive relief in return. The settlement would not require Ameritrade to return any fees that it acquired from its clients based on false pretenses about the security of its services. It would not require Ameritrade to give any assurance to class members that their sensitive information is being protected. It would not require Ameritrade to make any effort to warn its clients about the breach or the corresponding risk of identity theft. And it would not only fail to remedy Ameritrade's continuing falsehoods and misrepresentations about the breach, it would further perpetuate those misrepresentations by including them in a class notice that falsely characterizes the nature of the class's claims. As a result, it is likely that many Ameritrade clients will never learn that their social security numbers were compromised or, if they have already suffered identity theft, that Ameritrade may have been the cause. Given these fundamental flaws, the court should deny approval of the settlement.

FACTUAL BACKGROUND

In November 2006, plaintiff Matthew Elvey began receiving spam email touting fraudulent stock deals. Elvey Decl. ¶ 8. The email was sent to an address he had created

exclusively for use with his Ameritrade account and that he had given to nobody but Ameritrade. *Id.* Elvey reported the spam to the company, which responded via email that it was "conducting a thorough investigation into this matter." *Id* ¶ 9. When, several months later, Ameritrade had still not resolved the problem, Elvey entered a new, unique address into his Ameritrade account that he was careful not to disclose elsewhere. *Id.* ¶ 10. Soon, he again began receiving copies of the same spam. *Id.* Once again, he warned Ameritrade of the problem, and once again Ameritrade assured him that it was investigating the matter. *Id.* ¶ 12.

What Ameritrade did *not* tell Elvey is that it had been receiving similar complaints from other clients since at least October 2005. *Id.*; Sweet Decl. ¶¶ 2-4; Winzig Decl. ¶¶ 2-8. Some of these clients, like Elvey, informed Ameritrade that spam was being sent to email addresses that only Ameritrade knew about, and that therefore Ameritrade must be leaking customer data. Sweet Decl. ¶¶ 5, 8; Winzig Decl. ¶¶ 2-4. For more than a year, Ameritrade had told these clients the same thing it was telling Elvey—that it was investigating the matter. Sweet Decl. ¶ 4; Winzig Decl. ¶¶ 4, 8.

Elvey approached proposed class counsel with the evidence he had assembled that Ameritrade was leaking his email addresses. Elvey Decl. ¶ 14. In May 2007, counsel filed suit against Ameritrade and, soon after, moved for a preliminary injunction that would have compelled the company to fully reveal the nature of the security breach and to provide adequate warning to its clients. At around the same time, a column in the magazine *Network World* highlighted more cases of email addresses leaking from Ameritrade's servers and noted the "huge" potential implications. Elvey Decl., Exh. 3. A discussion of the problem, and more complaints, also appeared on the prominent Internet technology forum Slashdot and on other blogs and message boards. *Id.*, Exh. 4, 6 (blog post stating that "[t]here has been some serious chatter about Ameritrade's (AMTD) platform being compromised in some way, including the fact that customers' accounts could be in jeopardy"). Still, Ameritrade said nothing.

Not until three and half months after this lawsuit was filed—almost two years after the first known client had demonstrated the breach to Ameritrade and shortly before the scheduled argument on the preliminary injunction motion—did Ameritrade finally send a notice to its

clients, admitting for the first time that it had suffered a security breach involving the loss of client data. Defs.' Resp., Exh. 1 at 3. Even then, the company continued to be evasive, headlining its press release with the bold-faced statement: "You do not need to make any changes to your TD AMERITRADE accounts." *Id.* The company buried the fact that social security numbers were exposed in the middle of the notice, surrounding it with reassuring statements that the company had "no evidence" that such information was taken. *Id.* The notice did not mention that other data, including at least birth dates, names, phone numbers, addresses, and account numbers, were also exposed. Def.'s Resp., Exh. 1 at 1. The few news stories that covered the breach repeated Ameritrade's claim that no social security numbers were taken and that the problem was limited to a "spam issue." *See, e.g.*, *Customer Data Stolen from TD Ameritrade Database*, eWeek, Sept. 14, 2007. The company did not even attempt to explain why hackers with long-term access to its database would take only email addresses and leave much more valuable data behind.

What seems to have been largely lost on the media was the huge scope of the breach. With the records of six million customers exposed, Ameritrade's data breach was one of the largest in U.S. history and, given the nature of the exposure, perhaps the worst breach ever to have occurred. Just in terms of the number of affected people, Ameritrade's breach is the eighth largest recorded U.S. breach. *See* Open Security Foundation, *Largest data loss incidents*, http://datalossdb.org/index/largest (last visited July 8, 2009). Most large breaches, however, do not involve the loss of highly private information, such as social security numbers and dates of birth. Only three reported incidents in the U.S. involved the exposure of more than six million Social Security Numbers. *See id.* The first and largest occurred in 1984, before the phenomenon of identity theft had become an issue of national concern and before most states had enacted laws protecting the privacy of customer data. *Id.* The next breach was the widely reported loss of a Department of Veterans Affairs laptop in a burglary that contained the private information of 26.5 million veterans. *Id.* Although the stolen laptop was later recovered intact, the Department agreed to pay individual veterans between $75 and $1,500 for their exposure to identity theft. Hope Yen, *VA agrees to settle for $20M for data theft*, http://www.msnbc.msn.com/id/28880494/

(last visited July 9, 2009). In another case, the Bank of New York Mellon lost backup tapes containing private customer information. There was no evidence that anyone had found the tapes or misused the data, but in a settlement with Connecticut the bank agreed to provide notice to all affected customers, pay for 36 months of credit monitoring, and reimburse anyone whose funds were stolen as a result of the breach. State of Connecticut Dep't of Banking, *Department of Consumer Protection and Department of Banking Announce Settlement with Bank of New York Mellon*, http://www.ct.gov/dob/cwp/view.asp?a=2245&q=433242 (last visited July 9, 2009). Unlike these other breaches, which involved a one-time accidental loss of customer data, the evidence in this case indicates that Ameritrade's servers remained compromised for almost two years, and perhaps longer. Also unlike the other breaches, the evidence shows that Ameritrade was repeatedly warned over the entire period of exposure that a breach was underway even as it continued to assure customers that everything was fine. In these ways, Ameritrade's breach appears to be unprecedented.

Just one week after Ameritrade first announced the breach, the parties began settlement discussions. Hr'g Tr. June 12, 2008 ("Tr."), at 33. A few months later, before the Court had decided whether to certify the putative class, the parties reached a proposed settlement. The only discovery that had been completed was a deposition of Ameritrade's security chief, the transcript of which was designated "attorneys' eyes only." Tr. 19-20. Elvey Decl. ¶ 16. After a hearing on preliminary approval of the settlement, at which Elvey spoke against approval, proposed class counsel moved to withdraw as his representative. Elvey then retained the undersigned counsel and objected to preliminary approval of the settlement.

While this Court was considering the preliminary approval, the Texas Attorney General filed objections, arguing that the settlement would "confer minimal, if any, value to Class Members." The state raised numerous objections to the settlement terms, but, after several months of negotiations with the parties, informed the Court that it would withdraw its objections if certain minor conditions on the terms of the settlement were met. The changes requested by the Texas Attorney General were trivial and resolved none of the state's original complaints

about the settlement terms. Nevertheless, the settlement submitted by the parties failed to meet the state's conditions.

ARGUMENT

A district court may approve a settlement of a class action "only after a hearing and on finding that the settlement … is fair, reasonable, and adequate." Fed. R. Civ. P. § 23(e)(1)(C); *see Staton v. Boeing Co.*, 327 F.3d 938, 952 (9th Cir. 2003). The parties seeking approval bear the burden of showing that the settlement meets this standard. *Id.* The purpose of this requirement is "the protection of those class members including the named plaintiffs, whose rights may not have been given due regard by the negotiating parties." *Officers for Justice v. Civil Serv. Comm'n*, 688 F.2d 615, 624 (9th Cir. 1982).

The proposed settlement here requires a higher level of scrutiny because it was reached prior to class certification and at a time when proposed class counsel and Ameritrade were no longer in an adversarial posture. *See Amchem Prods., Inc. v. Windsor*, 521 U.S. 591, 620-21 (1997); *In re GM Corp. Pick-Up Truck Fuel Tank Prods. Liab. Litig.*, 55 F.3d 768, 787-88 (3d Cir. 1995); *Weinberger v. Great N. Nekoosa Corp.*, 925 F.2d 518, 520 (1st Cir. 1991). This is particularly true in light of the inherent tension attributable to class counsel's self-interest in achieving a settlement that, like this one, involves a substantial fee. *See Staton*, 327 F.3d at 959-60; *see also Powers v. Eichen*, 229 F.3d 1249, 1256 (9th Cir. 2000). Moreover, in-kind settlements, like the anti-spam software provided in this settlement, create a need for even more care, because the likely value of the settlement to class members is not apparent from the face of the settlement. *See Mars Steel Corp. v. Cont'l Ill. Nat'l Trust Co.*, 834 F.2d 677, 681 (7th Cir. 1984). Although this Court relied on the Texas Attorney General's participation in the process to create at least some kind of adversary process, the improvements it asked for would have had essentially no practical effect on the relief to the class and, in any case, were not all included in the settlement. There has still been almost no discovery in the case, and Texas's initial objection that the settlement would "confer minimal, if any, value to Class Members" remains just as true today.

The class's claims in this case assert that Ameritrade did not adequately protect sensitive client data, that it failed to warn its clients about a major security breach and the consequent risk of identity theft, and that it falsely claimed that its service was secure even long after it must have learned that hackers had obtained access. There are a variety of ways in which a fair settlement of these claims could have been reached, but any reasonable settlement would need to include some sort of remedy for the alleged harms. To address Ameritrade's misrepresentations about the quality of its security and its failure to live up to its fiduciary duty to deal honestly with its clients, Ameritrade should provide monetary relief to those who signed up for and used its services on false pretenses. Moreover, to address its failure to protect its customers' data, Ameritrade should agree to impose tighter security measures, protection against identity theft, adequate warnings about the breach, and corrective statements about the security of the company's servers.

As to all these forms of relief, however, the settlement makes only empty gestures. The settlement provides no monetary relief of any kind. Ameritrade promises to continue, for a few months, a small number of security practices that it is already voluntarily doing. Rather than protection against identity theft, Ameritrade agrees to institute an identity theft "claims process" under which those clients for which it has discovered direct evidence of identity theft resulting from the breach (so far, nobody, and likely to stay that way) are given a customer support phone number along with whatever other compensation Ameritrade decides, in its unfettered, unreviewable discretion, to give them. And rather than warnings or corrective statements, Ameritrade promises to post on its home page, during four one-week periods spread over the course of a year, a useless and generic statement that "warns" class members of nothing. Indeed, the settlement would provide even less than the year of free credit monitoring and 50 free trades that Ameritrade *voluntarily* gave to clients who complained about the problem. Elvey Decl., Exh. 7.

The only relief with any value in the case is addressed to only one consequence of the data breach—customers' receipt of spam resulting from the theft of client email addresses. The settlement would provide a one-year subscription to anti-spam software, a form of relief that, as

explained below, would be useless to many class members and which Ameritrade has apparently obligated itself to acquire even in the absence of a settlement. Not only is this relief nominal, it is tangential to the core issues in the case. By focusing all its relief on the software, the settlement buys into Ameritrade's mischaracterization of the security breach as a "spam issue."

Aside from the inadequacy of the proposed relief, three other features render it unfair to the class. First, the settlement provides for $1.87 million in attorneys' fees, which, given the paltry nature of the class relief, makes counsel the primary beneficiary of the agreement. Second, it releases Ameritrade from a range of claims that were not even asserted in this case and that are the only claims on which class members have a realistic chance of obtaining relief. Third, the class notice would further propagate Ameritrade's misleading characterizations of the breach by disclosing only the claims related to spam and by misrepresenting the terms of both Ameritrade's release from liability and the relief offered to the class. Under these circumstances, the parties have not, and cannot, meet their burden of demonstrating that the settlement is fair. For these reasons, the Court should deny approval of the settlement.

I. The Settlement Provides No Remedy for Identity Theft Resulting from Exposure of Social Security Numbers and Other Sensitive Data.

The core problem with the settlement is that it offers nothing of value to the class. As the Texas Attorney General noted in its objections, the settlement "purports to provide at least some relief to class members, but, in fact, the sum of the components provide little or no value." The settlement filed in response to Texas's complaints, however, does nothing to resolve the problem. The best that can be said about the amendments obtained by the Texas Attorney General is that they clear up some marginal ambiguities and extend the period during which class members can receive benefits that are essentially worthless. At the same time, however, the settlement still broadly waives the claims of class members while providing them with no relief.

A. Ameritrade's Data Breach Exposed Sensitive Customer Data Other Than Email Addresses.

As proposed class counsel have conceded, the issue of stolen email addresses and resulting spam is only one aspect of this case. Pls.' Resp. at 6 ("Foremost, the Settlement

addresses identity theft."); Tr. 10-11. In actuality, the scope of the data breach went far beyond email addresses, giving hackers access to the sensitive data of six million Ameritrade clients, including social security numbers, birth dates, account numbers, phone numbers, and addresses. Def.'s Resp., Exh. 1 at 1. This data includes the types of personal information (name, address, date of birth, and social security number) that are collectively known as a "full identity" and that are prized on the black market for their versatility. *See* Symantec Enterprise Security, *Symantec Global Internet Security Threat Report*, April 2008, at 17-19, 81, http://eval.symantec.com/ mktginfo/ enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiii_04-2008.en-us.pdf ("Threat Report"). In the hands of a thief, a person's full identity can cause far more harm than an email address: "With a full identity, a criminal can easily obtain government issued documents, commit credit card fraud, open bank accounts, obtain credit, purchase and/or steal homes, or even evade arrest by masquerading as someone else." *Id.*[1]

The parties have attempted to direct attention away from the fact that social security numbers were exposed to the question whether Ameritrade's consultant, ID Analytics, has detected "organized misuse" of this data. However, the parties have made no effort to demonstrate the relevance or scientific validity of the company's methodology, or even really to explain what that methodology is. *See, e.g.*, Tr. 13. There are no reported cases in which an ID Analytics report was accepted into evidence, and because the parties have kept the company's reports confidential, Tr. 39, there is no way for class members to effectively examine or rebut the company's conclusions. Moreover, the ID Analytics declaration submitted by Ameritrade does not justify the level of enthusiasm that the parties have expressed for it. The declaration states that the company "analyzed a subset of identity elements of consumers identified by TD Ameritrade," but does not identify the "subset" of information or the consumers identified. Cook Decl. ¶ 10. It concludes from this data only that "[w]ithin the ID Network, for this specific period

[1] Ameritrade has never said when the breach began or explained exactly what kinds of data were exposed, so the scope of the breach may have been even worse than is now known. As explained in part VII, the Court should not approve any settlement until Ameritrade has disclosed the full nature of the security breach to its clients.

and for this population of consumers, ID Analytics found no evidence of organized identity theft." *Id.* Unlike the parties, ID Analytics asserts no opinion, much less an opinion with a reasonable degree of scientific certainty, that its failure to find evidence of organized identity theft proves that identity theft has not or will not occur. Indeed, it expressly disclaims any predictions about whether the class members will face identity theft in the future.[2]

On the other hand, the very fact that hackers had long-term access to a database containing such valuable forms of private data is a strong reason to believe that the data was in fact stolen. A person's "full identity," according to one recent report, sells for about $1 to $15 on the underground market. Threat Report at 12. Email addresses, alone, on the other hand, sell for $.83 to $10 per *megabyte*, meaning one full identity is likely worth more than thousands of email addresses combined. *Id.* Under these circumstances, Ameritrade's claim to have no evidence that social security numbers were taken is no different than if it had claimed, after watching armed robbers coming out of an open bank vault, to have "no evidence" that any money was stolen. The company's claim of ignorance is especially unimpressive given that Ameritrade said the same thing about email addresses for almost two years while its clients were providing it with exactly the evidence it claimed it did not have.

B. The Security Policies Mandated by the Settlement Require Nothing of Ameritrade.

In response to the data leak, the settlement agreement specifies that Ameritrade will perform two kinds of security tests—account seeding, which creates dummy accounts to help track down the source of a breach, and penetration tests, which simulate a hacker's attempt to break into its system—and that it will employ ID Analytics to test for organized misuse of the data. Agmt. § IV(A)(2), (3), (5). The settlement also goes out of its way, however, to make clear that the company is already doing these things and would be doing them even in the absence of a

[2] Elvey has particular reasons to doubt the effectiveness of the methods used by ID Analytics. Since the breach has become public, four accounts have been fraudulently opened in his name. When he ordered a report on his risk of identity theft from ID Analytics, the company informed him that his risk of was low.

settlement. The agreement provides that Ameritrade will "continue" the specified practices, noting particularly that account seeding is "currently is in place" and that it "has retained" ID Analytics, whose analyses "have already been performed." *Id.* Indeed, as to ID Analytics, the settlement provides that Ameritrade must only finish out its *existing contract* with the company, something that, presumably, it is already obligated to do. *Id.* § IV(A)(5). The settlement does not require Ameritrade to adopt *any* new security measures to remedy the problems giving rise to the lawsuit, or even to reveal what those security problems were and how it has fixed them. *See Jamison v. Butcher and Sherrerd*, 68 F.R.D. 479, 482 (E.D. Pa. 1975) (refusing to approve a settlement where the class received nothing more than what it had already received in a prior settlement).

The settlement waters down these provisions even more by specifying that Ameritrade is obligated to continue doing what it is already doing for only a brief period of time. As for penetration tests, the company promises to conduct "bi-annual" testing, but only through December 31, 2009, which renders the provision meaningless. *Id.* § IV(A)(2). Account seeding is required to continue through the end of June, 2009, a date that has already passed, and the settlement further provides that the company "may change the methodology as it deems appropriate, provided the new method is no less rigorous than the one that currently is in place." *Id.* § IV(A)(3). After these short periods expire, Ameritrade is free to return to whatever lax security policies it chooses, effectively eviscerating whatever value these security practices may have had. *See Schwartz v. Dallas Cowboys Football Club, Ltd.*, 157 F. Supp. 2d 561, 573 (E.D. Pa. 2001) (finding the value of settlement's injunctive relief to be "minimal at best" where it would remain in place for only 1-2 years).

In any case, the specified security measures are well below the minimum of what would be expected from any financial services company. Elvey Decl. ¶ 21. As the Texas Attorney General stated in its objection to the settlement, the measures are "security practices in which any reputable company should engage, even if not the subject of litigation resulting from a security breach" and that Ameritrade would be obligated by law to adopt them even in the absence of a settlement. To have any real impact on the security of client data, the settlement

would have to provide for a set of best practices modeled on an existing industry standard. These practices would include, at least, a written security plan, a security audit to detect existing vulnerabilities, and periodic reassessment audits to ensure security is maintained. *Id.* ¶ 26. They would also include security controls such as encrypting and limiting access to high-risk data. *Id.* The Federal Trade Commission's settlement with TJX provides one possible model of what such an agreement would look like. *See* http://www.ftc.gov/os/caselist/ 0723055/ 080327agreement. pdf. That agreement provides for the company to adopt a comprehensive security program and requires bi-annual security audits by an independent security expert, as well as reporting to the FTC. *Id.* In addition to similar measures, a fair settlement would address one of the core problems giving rise to this case by providing a way for clients to report security vulnerabilities so that they would be acted upon instead of ignored.

C. The Settlement's "Claims Process" Is Worthless.

In the event that ID Analytics detects organized misuse of customer data, the settlement provides for a "claims process" through which those who have been identified as possible victims "are given the opportunity to submit claims to the Company." Agmt. § IV(A)(7). The process provides that Ameritrade will make available to these class members "dedicated customer support assistance trained to remediate any harms from identity theft." *Id.* § IV(A)(7)(a). Clients are also given the option of submitting a claim to Ameritrade, to which the company is free to offer compensation—or not—in any amount it deems reasonable. *Id.* § IV(A)(7)(b)-(c). If clients are not satisfied with Ameritrade's resolution of the problem, the claims process provides that they "may submit a claim in a binding arbitration." *Id.* § IV(A)(7)(d).

Proposed class counsel touts this system as one of the most important aspects of the settlement. Tr. 33-34. In actuality, it provides class members with nothing. Ameritrade has admitted that it would offer customer service to its clients even in the absence of the settlement agreement. Tr. 30-31. Indeed, Ameritrade's website reveals that it is *already* offering special customer service related to identity theft. The website states that the company has "a designated team responsible for reviewing potential threats to clients' assets and information," and advises

those who suspect they may be victims of identity theft to call the company, where "Client Services representatives are trained to help you." *See* http://www.tdameritrade.com/security/knowTheThreats/knowTheThreats.html; http://www.tdameritrade.com/security/knowTheThreats/securityIssue.html. The remainder of the process is equally pointless. Ameritrade clients do not need the benefit of a settlement agreement to ask the company for compensation that it can grant or deny in its discretion, and, as the agreement makes clear, the option of submitting disputes to binding arbitration is already "provided in the customer agreement with the company." Agmt. § IV(A)(7)(d).

Even if the process were potentially useful, it would still not benefit class members because it is unlikely that this portion of the settlement agreement would ever come into play. The settlement only obligates Ameritrade to provide customer support to "Identified Class Members," which it defines as "Settlement Class members whose information may have been subject to organized misuse." *Id.* § IV(A)(6). Ameritrade, however, "will have no such obligation if no organized misuse is detected by ID Analytics." Agmt. § IV(A)(7)(a). In other words, the company is not even required to provide customer service unless ID Analytics detects evidence of large-scale identity theft of Ameritrade's customers. Because ID Analytics has *already said* that it has found no evidence of organized misuse, the only way class members would benefit from this provision is if ID Analytics were to, for some reason, change its mind before the contract is up.

The Texas Attorney General recognized all these problems and objected to the settlement for these reasons, the modifications it has obtained to the terms on this issue, if anything, make things even worse. The agreement now says that class members are "entitled" to "the option to request from the Company compensation direct compensation of any identity-theft related costs." But Ameritrade customers would be "entitled" to "request" compensation regardless of whether there is a settlement. To further drive home the point, the settlement now describes the benefits do to the class as "[v]oluntary." Texas also asked that the settlement include a definition of the term "organized misuse" and provide "*all* Settlement Class Members, not just Identified Class Members, with dedicated customer support." Neither of these changes—of dubious value to

begin with—are included in the settlement. Rather than defining "organized misuse," as Texas had requested, the settlement defines "organized identity theft," a phrase that is not used anywhere of importance in the settlement. The parties did apparently acquiesce to Texas's request that the "claims period" be increased from thirty to ninety days, but Ameritrade always has discretion to give compensation regardless of whether the claims period has expired.

II. The Settlement Provides No Remedy for Ameritrade's Failure to Notify Its Customers of the Breach and to Falsely Advertise the Security of Its Services.

A major focus of the complaint is that Ameritrade took no action to notify its clients of its security breach, despite ample evidence of such a breach, and that the company engaged in deceptive trade practices by continuing to tout the strength of its security while omitting the material fact that it was in the midst of a major security breach. Just as the settlement provides no remedy for Ameritrade's exposure of sensitive customer data, it provides no remedy for these claims either.

A. Ameritrade Failed to Adequately Disclose the Breach to Its Customers and Prospective Customers.

There is little doubt that Ameritrade was aware of its security breach long before it finally admitted to it in September 2007. Ameritrade did not receive just one or two isolated complaints about the breach; since 2005, multiple clients provided it with both clear warnings and conclusive proof that it was leaking customer email addresses, all while Ameritrade continued to assert that it was "investigating" the matter. It is impossible to believe that Ameritrade could have failed to discover in a twenty-three-month investigation what Elvey was able to demonstrate in a matter of days—that spammers were somehow getting access to private customer email addresses. Even after a magazine article and prominent online technology forum exposed the data leaks, and even after the complaint in this lawsuit detailed proof of the breach, Ameritrade said nothing. Elvey Decl., Exh. 3-4. It was not until shortly before the argument date for plaintiffs' preliminary injunction motion, in which plaintiffs asked that Ameritrade be forced to notify its clients of the breach, that the company finally admitted it had a problem.

As plaintiffs convincingly argued in their motion for a preliminary injunction, Ameritrade's failure to disclose the security breach, a fact relevant to the agency relationship between Ameritrade and its clients, violated the company's fiduciary duty. The failure to disclose would also state a strong claim under the California Data Protection Act, Cal. Civ. Code § 1798.82, which provides that any company doing business in California must disclose security breaches after "discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person." A nearly two-year delay in admitting the breach is not made "in the most expedient time possible" as required by the Act. *Id.* [3]

Moreover, class members appear to have relatively straightforward claims for fraud or false advertising. Ameritrade's claims that its servers were subject to a high level of security—at a time when it was actually suffering an ongoing breach—was a misrepresentation about a material fact that would have misled any reasonable consumer about the advisability of signing up for an Ameritrade account. At the very least, Ameritrade had strong evidence that its customer data was not secure over a nearly two year period, during which it continued to reassure clients that everything was fine. Such a material misrepresentation of fact would give rise to common-law claims for fraud, under which Ameritrade's client should be entitled to a refund of fees paid under false pretenses, and would also implicate many state unfair competition laws that provide for statutory damages. As to these claims, Ameritrade's continued insistence that there is "no evidence" that Social Security Numbers were misappropriated is beside the point, because class members are entitled to know if there is even a risk that hackers took their highly sensitive data so they can make up their own minds about appropriate precautions. Ameritrade does not have to be able to prove that social security numbers were taken to inform its clients that they are at risk of identity theft. It is doubtful that even a single new client would

[3] Ameritrade argues that it would be very difficult to prove damages common to the class resulting from identity theft. Even assuming this is true, it would only increase the importance that the class receive injunctive relief. *See Walters v. Reno*, 145 F.3d 1032, 1048 (9th Cir. 1998); *Gilder v. PGA Tour, Inc.*, 936 F.2d 417, 423 (9th Cir. 1991).

have signed up for Ameritrade's service if the company had honestly revealed that the client's private information would be made available to unknown hackers.

Even now, Ameritrade has *still* not given adequate notice to its clients that they may be at risk of identity theft. The company's only statements on the matter have portrayed the breach as a "spam issue," burying the fact that sensitive data was in the targeted database while repeatedly claiming that it has "no evidence" this data was taken. There is still no notice of the breach *anywhere* on Ameritrade's customer website, even though the site continues to tout Ameritrade's "leading-edge" security systems. https://wwws.ameritrade.com/html/security_statement.html. Ironically, the website acknowledges that "awareness . . . can help to decrease the risk to your accounts and information," advising clients whose online security has been compromised to take precautions, while, at the same time, failing to mention that those reading the site are *themselves* likely at risk. http://www.tdameritrade.com/security/knowTheThreats/knowTheThreats.html. If anything, the website seems designed to conceal the data breach from Ameritrade's clients.

B. The Required "Warning" on Ameritrade's Website Is Not a Warning at All.

Perhaps the most disturbing aspect of the proposed settlement is that it would waive all the class's claims regarding the security breach without requiring Ameritrade to provide proper notice that the breach even occurred. The only aspect of the settlement that is even potentially relevant to this problem is the requirement that Ameritrade place a so-called "warning" on its website. Agmt. § IV(A)(1). The language of the required statement, however, sounds more like general background information than an important warning to Ameritrade clients. *Id.* ("Go to Security Center for important information on protecting your assets from online threats such as identity theft, phishing, spyware, viruses, email fraud, and stock touting spam.").

Moreover, the settlement includes no requirements regarding what clients will see when they click on the link, providing only that it will be "a warning to customers regarding stock spam." *Id.* The agreement does not require that Ameritrade warn customers about the *particular* stock scams to which its clients have been subjected, that Ameritrade is responsible for leaking clients' email addresses, or that their social security numbers have been exposed to hackers. General background information may be useful, but any general notice about stock spam that

fails to mention that Ameritrade customers are at particular risk would, by omitting a material fact, be itself misleading.

Finally, the "warning" seems designed so that it will be read by as few class members as possible. The settlement provides that it be posted on Ameritrade's website for "one week at a time, four times during a 12 month period," requiring it to be put up and taken back down four times over the course of a year. *Id.* The Texas Attorney General objected to the settlement on this basis, noting that, "except for four weeks out of the year, the information will be wholly buried in 'The Security Center' portion of Defendant's Web site, which is unlikely to be visited by the type of consumer must vulnerable to stock scams," but now appears to have dropped this objection. Nevertheless, there is no legitimate basis for this provision—which actually requires more work by Ameritrade—other than to conceal the warning from Ameritrade clients.

To give class members any real relief on the failure to warn and false advertising claims, the settlement should provide for Ameritrade to fully disclose to the class the nature of the breach, exactly what forms of data were exposed, what the company has done to resolve the problem, and what clients can do to protect themselves from identity theft. The company should provide this information in the form of personal notice by email or regular mail, as well as a long-term conspicuous statement on its website. An example of a warning statement that would provide adequate notice to the class is suggested in plaintiffs' motion for a preliminary injunction. Such a notice would go a long way toward protecting the class's interests. Moreover, the company should offer compensation to clients who relied on its misrepresentations in deciding to utilize the service.

III. The Value of the Spam-Blocking Software Does Not Render the Settlement Fair.

Although spam is only one aspect of this case, it is the target of the only relief of any possible value: a one-year subscription to Trend Micro Internet Security Pro anti-spam software. The provision of this software does not render the settlement fair. The Court has a responsibility "to ensure that the settlement provides real value" by offering relief that the class will actually use. *Sylvester v. Cigna Corp.*, 369 F.Supp.2d 34, 49 (D. Me. 2005); *see also* 2003 Advisory Committee Notes, Fed. R. Civ. P. 23(h) ("Settlements involving nonmonetary provisions for

class members also deserve careful scrutiny to ensure that these provisions have actual value to the class."). Here, the settlement would leave many class members without any relief. The software will be worthless to the many class members who already have anti-spam software or who use popular online email clients like Gmail, Yahoo!, and Hotmail that are free of charge and have anti-spam capabilities built in. Moreover, many class members will have already changed their email addresses, either because they have been deluged with spam related to the data breach or for some other reason. Although the software will not be completely without value to these class members, they will no longer be able to use it for its intended purpose: to block the fraudulent spam caused by Ameritrade's data breach. These class members will thus have little or no incentive to obtain the software. *See In re Gen'l Motors Corp. Engine Interchange Litig.*, 594 F.2d 1106, 1130-31 (7th Cir. 1979) ("The federal claims of individual class members cannot be extinguished with neither adequate consideration in return nor a hearing on the merits of their claims.").

The Texas Attorney General recognized the lack of value in this aspect of the settlement, objecting on the ground that "the vast majority of Internet users have access to free subscriptions to similar security software through their Internet Service Provider" and therefore that "it is unlikely that any significant portion of the class will realize any value from the coupon for security software." Nevertheless, Texas withdrew its objection after achieving only one improvement to the settlement in this area—that the unique identifier number used to download the software "will be valid until at least January 1, 2010." If the relief has no value, an extended opportunity to take advantage of that relief is not an improvement. Moreover, although the full notice states, on page 2, that "the software must be downloaded by January 1, 2010," the summary notice omits this fact. Thus, class members will more than likely not be put on notice of the deadline.

Because the settlement requires class members to log into a website to download the software rather than requiring Ameritrade to them, the value of the settlement is further reduced. Experience has shown that recovery rates drop dramatically when class members are required to take additional steps to obtain their recovery. *See Buchet v. ITT Consumer Finance Corp.*, 845

F.Supp. 684, 693-96 (D. Minn.1994), *amended*, 858 F.Supp. 944 (discussing how the likely rate of coupon redemption affects the settlement's value to the class). Downloading the software may be extremely inconvenient for those class members who lack a broadband Internet connection and are forced to spend hours downloading it over a phone line. Although the parties bear the burden of providing a valuation for the settlement on which a reasonableness determination can be based, they make no effort to determine what percentage of the class would likely download the software, making accurate valuation of the settlement impossible. *See In re GM Corp. Pick-Up Truck*, 55 F.3d at 808 (settlement was not adequate, among other reasons, because use of supplied coupons during the redemption period would have been difficult).[4]

The cost of the software to Ameritrade is itself very low, requiring Ameritrade to pay $6 million for the right to distribute the software to its clients, or about $1 for each of the approximately six million class members. That number may also be deceptive, however, because it appears that Ameritrade may have a preexisting relationship with Trend Micro that, although already established, it is now attempting to claim as a benefit of the settlement. According to the declaration of Trend Micro's sales manager, Ameritrade's $6 million contract with the company allows it to distribute copies of the software between December 2007 and March 2011, meaning that Ameritrade *already has* a deal with Trend Micro that allows it to distribute software even though the settlement is not finalized. Thomas Decl. ¶ 11. Ameritrade seems to admit this in its brief, stating that it has already "locked in" the price of the software. If Ameritrade is benefitting from this arrangement with Trend Micro, or if it would have entered into the contract regardless of the settlement, that would provide further reason to find that the settlement is not fair, adequate, or reasonable.

[4] Redemption rates in class action cases are often 10% or less. *See, e.g., In re Compact Disc Minimum Advertised Price Antitrust Litig.*, 370 F. Supp. 2d 320, 321 (D. Me. 2005) (2% submission rate); *Buchet*, 845 F.Supp. at 695 (rejecting settlement with 3% redemption rate); *Strong v. Bellsouth Telecomm., Inc.*, 173 F.R.D. 167, 169 (W.D. La. 1997), aff'd, 137 F.3d 844 (5th Cir. 1998) (4.3% claims rate).

Finally, even setting aside its nominal value to some class members, the anti-spam software makes no sense as the primary relief for plaintiffs' claims because it includes no relief relevant to the core issues in the complaint. Although it was spam that originally drew Elvey's attention to the security breach, to direct all relief toward spam while ignoring the breach itself is to confuse the symptom with the disease. Without injunctive relief requiring improvements in Ameritrade's security practices or accurate notice to the class, the provision of the software does not make the settlement any more fair.

IV. The Proposed $1.8 Million Fee Further Undermines the Settlement's Fairness.

Unlike the class relief, which is non-monetary and contingent on class members downloading the software, the settlement provides for class counsel to receive $1.8 million in attorneys' fees, regardless of how few class members ultimately obtain the software. Agmt § IX. The amount of requested attorneys' fees is an important factor in assessing the reasonableness of class relief, since every dollar that goes to class counsel is a dollar less that could have been used to compensate class members. Even when the terms of the settlement provide that attorneys' fees are paid by the defendant, "those fees are still best viewed as an aspect of the class's recovery." *Johnson v. Comerica*, 83 F.3d 241, 246 (8th Cir. 1996). "[I]n essence the entire settlement amount comes from the same source. The award to the class and the agreement on attorney fees represent a package deal." *Id.*; *see also Great N. Nekoosa*, 925 F.2d at 522.

Because the parties have not provided any way to accurately judge the value of the in-kind relief to the class, it is impossible to determine the reasonableness of fees by reference to the value of the settlement. There are particular reasons, however, to be suspicious of the fees here. First, the provision of a fee to which the defendant has agreed creates the risk that class counsel may have bargained away valuable relief "in exchange for red carpet treatment on fees." *Weinberger v. Great N. Nekoosa Corp.*, 925 F.2d 518, 524-25 (1st Cir. 1991). Second, "the fact that the settlement involved non-cash relief only . . . is recognized as a prime indicator of suspect settlements." *In re GM Corp. Pick-Up Truck*, 55 F.3d at 80. And third, because the proposed attorneys' fees are not linked to how much relief is actually obtained by the class, there is no

incentive for class counsel to ensure that the class obtains any relief with actual value. *See Polar Int'l Brokerage Group v. Reeve*, 187 F.R.D. 108, 119-20 (S.D.N.Y. 1999).

In this context, the $1.8 million fee provided by the settlement is excessive in relation to the minimal value of the relief. *See In re GM Corp. Pick-Up Truck*, 55 F.3d at 803 (holding fees excessive where "the settlement did not maximize the class members' interests"). This is especially true given that proposed class counsel limited its discovery to a single deposition, relied primarily on evidence provided by Elvey, and took little risk in laying out total expenses of $9000. *Id.* ("[C]lass counsel effected a settlement that would yield very substantial rewards to them after what, in comparison to the $9.5 million fee, was little work."); Agmt. § IX.

Nor has counsel shown that its lodestar figure is reasonable. It is impossible to judge the fairness of the fees claimed by counsel given that they did not submit detailed time records. *See In re Wash. Pub. Power Supply Sys. Secs. Litig.*, 19 F.3d 1291, 1305-06 (9th Cir. 1994) ("The party petitioning for attorneys' fees bears the burden of submitting detailed time records justifying the hours claimed to have been expended.") (internal quotation omitted). For example, there is no way without detailed time records to determine whether certain hours were unnecessary, excessive, or duplicative. *Id.* (holding that hours may be reduced for these reasons). Moreover, if, as appears to be the case, a substantial fraction of counsel's time was devoted to negotiating their own fees rather than negotiating benefits for the class, the lodestar fee may also be excessive for that reason. *Id.* at 1299 (holding that time spent negotiating fees in common fund cases is not compensable).

V. The Scope of the Released Claims Is Far Too Broad.

The broad scope of the release, which waives the class's right to bring claims that were not even asserted in this case, is another reason why the proposed settlement is unfair. The agreement specifies that the class waives all right to bring any class claims against Ameritrade that were or *could have* been brought in this case, except for individual claims for identity theft. This release is too broad because it is not limited to claims arising out of the subject matter of this case. Class members should not be required to waive their right to bring other actions against Ameritrade to settle their claims regarding this particular breach. *See* Rossman & Edelman,

Consumer Class Actions § 12.3.3 (2006) at 165 ("Plaintiffs' counsel should not allow any release phrased in vague terms, such as 'all claims which could have been brought.'"). Class counsel did not purport to represent the class on these claims, and therefore cannot now release them. *See Nat'l Super Spuds v. N.Y. Merc. Exchange*, 660 F.2d 9, 18-20 (2d Cir. 1981).

The Texas Attorney General focused many of its objections on the problems with the scope of the release, but the proposed settlement does not resolve these problems. The agreement now provides that claims are not released against those who actually committed the data theft and that claims of government entities are not released, but these are peripheral issues and it is doubtful that any court would have held these claims released anyway. Indeed, Ameritrade has no authority to release the claims of government entities who are not parties to the case. Although the settlement previously purported to preserve any individual class member's "claim for identity theft," the settlement now preserves "any claims for damages caused by identity theft." Although it is helpful to clarify the meaning of "claim for identity theft" (because there is no recognized cause of action for "identity theft"), the release would still abandon class members' individual claims against Ameritrade for failing to notify them of the breach and for falsely advertising the security of its services, which appear to be the only claims in the case likely to lead to significant damage awards. Moreover, because the settlement now specifies that the preserved claims are "for damages," it would preclude any possibility of future injunctive relief.

VI. The Notice Would Further Deceive Class Members by Misrepresenting the Nature of the Claims and Relief.

Due process requires that absent class members receive notice of material terms of class settlements. *Mullane v. Cent. Hanover Bank & Trust Co.*, 339 U.S. 306, 313 (1950). Far from providing such notice, the settlement here perpetuates Ameritrade's misrepresentation of the data breach as a "spam issue," leaving class members in the dark about what claims they are asserting and giving away. The notice describes the complaint as "alleg[ing] that an unauthorized third party acquired e-mail addresses of the Company's accountholders that were then used by spammers to send unsolicited commercial emails promoting certain stocks." There is no mention

of the other claims in the complaint, including the allegations that social security numbers and other sensitive data were also exposed. Nor does the notice mention that the class is asserting claims for breach of fiduciary duty and unfair competition, or that the class is releasing these claims along with any other claims that *could have* been brought in the litigation. These characterizations are particularly misleading because, by treating the case as one about spam, the notice makes the only real relief in the case—the anti-spam software—appear much more reasonable than it actually is.[5]

The summary notice to be sent to class members, by omitting key details about the relief as described in the full notice, is even more misleading. The notice states that the settlement provides "additional measures to protect the privacy of client information," when in fact Ameritrade is *already* providing all the required security measures. It also describes the required statement on Ameritrade's website as a "warning," even though the actual message does not warn class members about anything. Although a summary notice may be able to omit technical or unimportant details of a settlement for purposes of readability, this notice omits material facts to give the impression that Ameritrade will institute serious security improvements and provide real warnings to the class—provisions that, had they actually been included in the settlement, would have made it much more palatable.

The only relevant change to the terms of the notice added after negotiation with the Texas Attorney General is an unexplained reference to "the data breach," which, in context, appears to refer only to the loss of email addresses. There is no mention anywhere of social security numbers, dates of birth, or any other information. This falls far short of the changes Texas demanded as a condition of withdrawing its objections: "Providing an explanation of the basis of the suit that includes the fact that TD Ameritrade's computer database suffered a data security breach and exposed the Class Members to the risk of identity theft." Moreover, after negotiations

---

[5] The notice also continues to downplay the extent of the breach by repeating, in bold letters, Ameritrade's misleading claim that there is "no evidence of organized misuse of personal information."

with Texas, the summary notice no longer contains the statement: "If you are a member of the Settlement Class and do not exclude yourself in the manner required, your claims against Defendant and its affiliates, their predecessors and successors will be released upon final approval of the settlement by the Court." Customers are therefore no longer warned that by doing nothing they will be waiving all their claims.

No matter their opinion on the strength of the cause of action, the parties have no excuse for failing to honestly describe the nature of the claims to those who will be giving them up. This is especially true given that notice is being provided by email and the cost of fully and clearly explaining the nature of the case is essentially free.

VII. The Fairness of the Settlement Cannot Be Determined Without Review of the Evidentiary Record in the Case.

The right of class members to be heard on the fairness and adequacy of a settlement includes an opportunity to develop the record supporting their objections, so that the settlement's adequacy can be tested through an appropriate, adversary process. *Girsh v. Jepson*, 521 F.2d 153, 157 (3d Cir. 1975); *Greenfield v. Villager Indus.*, 483 F.2d 824, 833 (3d Cir. 1973). Here, Ameritrade has kept most aspects of the breach secret and has refused the request of undersigned counsel to view the only discovery in the case—the single deposition of Ameritrade's security chief. The lack of any information about the breach other than Ameritrade's self-serving assertions prevents Elvey and other class members from evaluating key aspects of the case that bear on their decision whether to settle. To give Elvey and other class members the opportunity to challenge the propriety of the settlement, the Court should withhold approval and order the parties to file in the public record all information necessary to evaluate the settlement's fairness. This would include, at least, the record of the deposition, the reports by ID Analytics, any contracts with Trend Micro, information about the redemption rate for the anti-spam software, and any other evidence on which the parties intend to rely. Making the evidence public will ensure that some class members will not have preferential access to it while others, who have an equal interest in the material, are left in the dark. As the U.S. Court of Appeals for the Fifth Circuit recently observed, a process in which class members are "deprived of information

necessary to contest" a settlement because critical information is kept secret is "inherently flawed." *In re High Sulfur Content Gasoline Prods. Liab. Litig.*, 517 F.3d 220, 232 (5th Cir. 2008).

VIII. The Parties Should Not Be Allowed to Punish Elvey for His Objections by Withdrawing His Incentive Award.

As a final matter, the parties removed the settlement's award of $10,000 to Elvey after he objected to the fairness of the settlement. The only reason for this change is to punish Elvey for objecting to the fairness of the settlement. Elvey has been far more involved in this case than a typical named plaintiff, and is responsible for discovering the data breach and bringing it to class counsel's attention. If parties could take away a named plaintiff's incentive award for objecting to a settlement, it would create a strong incentive for them to keep silent, no matter how unfair the terms.

CONCLUSION

For the foregoing reasons, this Court should deny final approval to the proposed class settlement and should order the parties to file and serve on Elvey's counsel any evidence on which the parties have relied or intend to rely in support of the settlement's fairness.

Date: July 9, 2009

Respectfully submitted,

CHAVEZ & GERTLER, LLP

PUBLIC CITIZEN LITIGATION GROUP

/s/Gregory A. Beck_____
Gregory A. Beck, admitted pro hac vice

Attorneys for Plaintiff