

1 MARK A. CHAVEZ (SBN 90858)  
CHAVEZ & GERTLER, LLP  
2 42 Miller Ave.  
3 Mill Valley, CA 94941  
4 Telephone: (415) 381-5599

5 GREGORY A. BECK (To Be Admitted Pro Hac Vice)  
6 BRIAN WOLFMAN (To Be Admitted Pro Hac Vice)  
PUBLIC CITIZEN LITIGATION GROUP  
7 1600 20th St. NW  
8 Washington, DC 20009  
9 Telephone: (202) 588-1000

10 Attorneys for Plaintiff Matthew Elvey

11 UNITED STATES DISTRICT COURT  
12 NORTHERN DISTRICT OF CALIFORNIA

13 In re TD AMERITRADE ) Case No. C 07-2852 VRW  
14 ACCOUNTHOLDER LITIGATION )  
15 ) CLASS ACTION  
16 ) **PLAINTIFF MATTHEW ELVEY'S**  
17 ) **CORRECTED RESPONSE TO THE**  
18 ) **PARTIES' BRIEFS IN RESPONSE TO THE**  
19 ) **COURT'S JUNE 13, 2008 ORDER**  
20 )  
21 )  
22 )  
23 )  
24 )  
25 )  
26 )  
27 )  
28 )

**TABLE OF CONTENTS**

1

2

3 INTRODUCTION ..... 1

4 FACTUAL BACKGROUND ..... 1

5 ARGUMENT ..... 4

6 I. The Settlement Provides No Remedy for Identity Theft Resulting from  
Exposure of Social Security Numbers and Other Sensitive Data ..... 6

7 A. Ameritrade’s Data Breach Exposed Sensitive Customer Data Other  
Than Email Addresses. .... 6

8 B. The Security Policies Mandated by the Settlement Require Nothing  
of Ameritrade. .... 8

9 C. The Settlement’s “Claims Process” Is Worthless. .... 9

10

11 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  
12 Services. .... 11

13 A. Ameritrade Failed to Adequately Disclose the Breach to Its  
Customers and Prospective Customers. .... 11

14 B. The Required “Warning” on Ameritrade’s Website Is Not a  
15 Warning at All. .... 12

16 III. The Value of the Spam-Blocking Software Does Not Render the  
17 Settlement Fair. .... 14

18 IV. The Provision of a \$1.8 Million Fee Further Undermines the Settlement’s  
Fairness. .... 16

19 V. The Scope of the Released Claims Is Far Too Broad. .... 17

20 VI. The Defective Class Notice Provides an Independent Reason to Reject the  
21 Settlement. .... 18

22 A. The Notice Would Further Deceive Class Members by  
Misrepresenting the Nature of the Claims and Relief. .... 18

23 B. The Notice Is Poorly Designed to Reach Class Members or to  
24 Allow Them to Opt Out. .... 20

25 VII. The Fairness of the Settlement Cannot Be Determined Without Review of  
the Evidentiary Record in the Case. .... 21

26 VIII. Elvey’s Signature on the Settlement Agreement Should Not Affect this  
27 Court’s Analysis of His Objections. .... 21

28 CONCLUSION ..... 23

**TABLE OF AUTHORITIES**

**CASES**

1

2

3

4 *Amchem Prods., Inc. v. Windsor,*  
521 U.S. 591 (1997)..... 4

5

6 *Buchet v. ITT Consumer Finance Corp.,*  
845 F.Supp. 684 (D. Minn.1994)..... 14

7

8 *D.R.I., Inc. v. Dennis,*  
2004 WL 1237511 (S.D.N.Y. June 3, 2004) ..... 20

9

10 *Gilder v. PGA Tour, Inc.,*  
936 F.2d 417 (9th Cir. 1991) ..... 11

11

12 *Girsh v. Jepson,*  
521 F.2d 153 (3d Cir. 1975)..... 21

13

14 *Grant v. Bethlehem Steel Corp.,*  
823 F.2d 20 (2d Cir. 1987)..... 22

15

16 *In re Compact Disc Minimum Advertised Price Antitrust Litig.,*  
370 F.Supp.2d 320 (D. Me. 2005) ..... 14

17

18 *In re Gen'l Motors Corp. Engine Interchange Litigation,*  
594 F.2d 1106 (7th Cir. 1979) ..... 19

19

20 *In re GM Corp. Pick-Up Truck Fuel Tank Products Liability Litigation,*  
55 F.3d 768 (3d Cir. 1995)..... 4, 14, 16

21

22 *In re High Sulfur Content Gasoline Prods. Liab. Litig.,*  
517 F.3d 220 (5th Cir. 2008) ..... 21

23

24 *In re Washington Public Power Supply System Securities Litigation,*  
19 F.3d 1291 (9th Cir. 1994) ..... 17

25

26 *Johnson v. Comerica,*  
83 F.3d 241 (8th Cir. 1996) ..... 16

27

28 *Mars Steel Corp. v. Continental Illinois National Trust Co.,*  
834 F.2d 677 (7th Cir. 1984) ..... 4

1 **CASES (CONT'D.)**

2 *Mullane v. Central Hanover Bank & Trust Co.*,

3 339 U.S. 306 (1950)..... 18

4 *Nat'l Super Spuds v. N.Y. Merc. Exchange*,

5 660 F.2d 9 (2d Cir. 1981)..... 17

6 *Officers for Justice v. Civil Serv. Comm'n*,

7 688 F.2d 615 (9th Cir. 1982) ..... 4

8 *Piambino v. Bailey*,

9 610 F.2d 1306 (5th Cir. 1980) ..... 19

10 *Polar Int'l Brokerage Group v. Reeve*,

11 187 F.R.D. 108 (S.D.N.Y. 1999) ..... 16

12 *Powers v. Eichen*,

13 229 F.3d 1249 (9th Cir. 2000) ..... 4

14 *Schwartz v. Dallas Cowboys Football Club, Ltd.*,

15 157 F.Supp.2d 561 (E.D. Pa. 2001) ..... 8-9

16 *Staton v. Boeing Co.*,

17 327 F.3d 938 (9th Cir. 2003) ..... 4, 19

18 *Strong v. Bellsouth Telecommunications, Inc.*,

19 173 F.R.D. 167 (W.D. La. 1997) ..... 14

20 *Sylvester v. Cigna Corp.*,

21 369 F.Supp.2d 34 (D. Me. 2005) ..... 13

22 *Walters v. Reno*,

23 145 F.3d 1032 (9th Cir. 1998) ..... 11

24 *Weinberger v. Great Northern Nekoosa Corp.*,

25 925 F.2d 518 (1st Cir. 1991)..... 4, 16

26 **STATUTES AND RULES**

27 2003 Advisory Committee Notes,

28 Fed. R. Civ. P. 23(h) ..... 13

California Data Protection Act, Cal. Civ. Code

§ 1798.82..... 11

Fed. R. Civ. P.

§ 23(e)(1)(C) ..... 4

1 **OTHER AUTHORITIES**

2 *Customer Data Stolen from TD Ameritrade Database,*  
3 *eWeek, Sept. 14, 2007* ..... 3

4 *Paul McNamara, Judge Halts Ameritrade Settlement that Would Mean a Boon for*  
5 *Lawyers, a Pittance for Victims,*  
6 *Network World, June 16, 2008* ..... 22

7 *Rossman & Edelman, Consumer Class Actions*  
8 *§ 12.3.3*..... 17

9 *Symantec Enterprise Security, Symantec Global Internet Security Threat Report,*  
10 *April 2008, [http://eval.symantec.com/mktginfo/enterprise/white\\_papers/b-](http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiii_04-2008.en-us.pdf)*  
11 *whitepaper\_internet\_security\_threat\_report\_xiii\_04-2008.en-us.pdf*..... 6, 7

10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

1 **INTRODUCTION**

2 This is a proposed class action against TD Ameritrade (“Ameritrade”) over the  
3 consequences of a major security breach that allowed outside hackers access to sensitive client  
4 data on the company’s servers, including social security numbers, birth dates, and account  
5 numbers. Def.’s Resp. to June 13 Order (“Def.’s Resp.”), Exh. 1 at 1. This security breach was  
6 not an isolated loss of data; the hackers had continuous access for at least twenty-three months to  
7 the private data of six million Ameritrade clients. Sweet Decl. ¶ 2; Winzig Decl. ¶ 2. Despite the  
8 mounting evidence of a serious security breach, Ameritrade took no action to notify its clients of  
9 the problem or warn them that they may be at risk of identity theft. Only after plaintiffs asked the  
10 Court to order Ameritrade to disclose the breach did the company finally admit that  
11 “unauthorized code” on its systems had allowed outsiders to take “certain information” from its  
12 client database. Def.’s Resp., Exh. 1 at 3.

13 The proposed settlement would release the rights of the class to seek relief against  
14 Ameritrade for the breach without providing them with any monetary or injunctive relief in  
15 return. It would not require Ameritrade to give any assurance to class members that their  
16 sensitive information is being protected. It would not require Ameritrade to make any effort to  
17 warn its clients about the breach or the corresponding risk of identity theft. And it would not only  
18 fail to remedy Ameritrade’s continuing falsehoods and misrepresentations about the breach, it  
19 would further perpetuate those misrepresentations by including them in a class notice that falsely  
20 characterizes the nature of the class’s claims. As a result, it is likely that many Ameritrade clients  
21 will never learn that their social security numbers were compromised or, if they have already  
22 suffered identity theft, that Ameritrade may have been the cause. Given these fundamental flaws  
23 in the settlement—which provides no real relief relevant to any of the class’s core claims—the  
24 Court should deny preliminary approval.

25 **FACTUAL BACKGROUND**

26 In November 2006, plaintiff Matthew Elvey began receiving spam email touting  
27 fraudulent stock deals. Elvey Decl. ¶ 8. The email was sent to an address he had created  
28 exclusively for use with his Ameritrade account and that he had given to nobody but Ameritrade.

1 *Id.* Elvey reported the spam to the company, which responded via email that it was “conducting a  
2 thorough investigation into this matter.” *Id.* ¶ 9. When, several months later, Ameritrade had still  
3 not resolved the problem, Elvey entered a new, unique address into his Ameritrade account that  
4 he was careful not to disclose elsewhere. *Id.* ¶ 10. Soon, he again began receiving copies of the  
5 same spam. *Id.* Once again, he warned Ameritrade of the problem, and once again Ameritrade  
6 assured him that it was investigating the matter. *Id.* ¶ 12.

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

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

25 Not until three and half months after this lawsuit was filed—almost two years after the  
26 first known client had demonstrated the breach to Ameritrade and shortly before the scheduled  
27 argument on the preliminary injunction motion—did Ameritrade finally send a notice to its  
28 clients, admitting for the first time that it had suffered a security breach involving the loss of

1 client data. Defs.' Resp., Exh. 1 at 3. Even then, the company continued to be evasive, headlining  
2 its press release with the bold-faced statement: "You do not need to make any changes to your  
3 TD AMERITRADE accounts." *Id.* The company buried the fact that social security numbers  
4 were exposed in the middle of the notice, surrounding it with reassuring statements that the  
5 company had "no evidence" that such information was taken. *Id.* The notice did not mention that  
6 other data, including at least birth dates, names, phone numbers, addresses, and account  
7 numbers, were also exposed. Def.'s Resp., Exh. 1 at 1. At the same time it was issuing the press  
8 release, Ameritrade set up an automated phone message from CEO Joe Moglia assuring clients  
9 that "[i]t's a spam issue, but no accounts were touched. . . . User IDs and passwords remain  
10 protected. There is no evidence that SSNs were ever taken." *Customer Data Stolen from TD*  
11 *Ameritrade Database*, eWeek, Sept. 14, 2007. If Ameritrade had no evidence that social security  
12 numbers were taken, however, it also had no evidence that they were *not* taken. The company  
13 did not even attempt to explain why hackers with long-term access to its database would take  
14 only email addresses and leave much more valuable data behind.

15 About a week after Ameritrade made its announcement, the parties began settlement  
16 discussions. Hr'g Tr. June 12, 2008 ("Tr."), at 33. Elvey attempted to play an active role in the  
17 settlement process, stressing to his counsel that the company should at least be required to  
18 provide proper notice to its clients and to institute an internal security policy, backed by an  
19 independent security audit, that would protect client data in the future. Elvey Decl. ¶ 15.  
20 However, his participation was limited by the fact that he was not given access to any  
21 information about the breach. The only discovery completed in the case was a deposition of  
22 Ameritrade's security chief, the transcript of which was designated "attorneys' eyes only," Tr.  
23 19-20, and which Elvey has never been allowed to see. Elvey Decl. ¶ 16.

24 Nine months after the complaint was filed, and before the Court had decided whether to  
25 certify the putative class, Elvey's counsel presented him with a proposed settlement. *Id.* ¶ 17.  
26 The agreement included none of the key features Elvey had asked for, but when he complained  
27 of this he was told that it was too late to make substantive changes. *Id.* ¶ 18. After a hearing on  
28 preliminary approval of the settlement, at which Elvey spoke against approval, proposed class

1 counsel moved to withdraw as his representative. Elvey has now retained the undersigned  
2 counsel to press his objections to the proposed settlement's terms.

### 3 ARGUMENT

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

11 The proposed settlement here requires a higher level of scrutiny because it was both  
12 reached prior to class certification and when proposed class counsel and Ameritrade were no  
13 longer in an adversarial posture. *See Amchem Prods., Inc. v. Windsor*, 521 U.S. 591, 620-21  
14 (1997); *In re GM Corp. Pick-Up Truck Fuel Tank Prods. Liab. Litig.*, 55 F.3d 768, 787-88 (3d  
15 Cir. 1995); *Weinberger v. Great N. Nekoosa Corp.*, 925 F.2d 518, 520 (1st Cir. 1991). This is  
16 particularly true in light of the inherent tension attributable to class counsel's self-interest in  
17 achieving a settlement that, like this one, involves a substantial fee. *See Staton*, 327 F.3d at 959-  
18 60; *see also Powers v. Eichen*, 229 F.3d 1249, 1256 (9th Cir. 2000). Moreover, in-kind  
19 settlements, like the anti-spam software provided in this settlement, create a need for even more  
20 care, because the likely value of the settlement to class members is not apparent from the face of  
21 the settlement. *See Mars Steel Corp. v. Cont'l Ill. Nat'l Trust Co.*, 834 F.2d 677, 681 (7th Cir.  
22 1984).

23 The class's claims in this case assert that Ameritrade did not adequately protect sensitive  
24 client data, that it failed to warn its clients about a major security breach and the consequent risk  
25 of identity theft, and that it falsely claimed that its service was secure even long after it must  
26 have learned that hackers had obtained access. There are a variety of ways in which a fair  
27 settlement of these claims could have been reached, but any reasonable settlement would (at least  
28 in the absence of monetary relief) need to include some sort of remedy for the alleged harms,

1 such as better security for client data, protection against identity theft, adequate warnings about  
2 the breach, and corrective statements about the security of the company's servers. As to these  
3 forms of relief, however, the settlement makes only empty gestures. Rather than better security,  
4 Ameritrade promises to continue, for a few months, a small number of security practices that it is  
5 already voluntarily doing. Rather than protection against identity theft, Ameritrade agrees to  
6 institute an identity theft "claims process" under which those clients for which it has discovered  
7 direct evidence of identity theft resulting from the breach (so far, nobody, and likely to stay that  
8 way) are given a customer support phone number along with whatever other compensation  
9 Ameritrade decides, in its unfettered, unreviewable discretion, to give them. And rather than  
10 warnings or corrective statements, Ameritrade promises to post on its home page, during four  
11 one-week periods spread over the course of a year, a useless and generic statement that "warns"  
12 class members of nothing.

13 The only relief with any value in the case is addressed to only one consequence of the  
14 data breach—customers' receipt of spam resulting from the theft of client email addresses. The  
15 settlement would provide a one-year subscription to anti-spam software, a form of relief that, as  
16 explained below, will be useless to many class members and that will cost Ameritrade, at most,  
17 about \$1 each. Not only is this relief nominal, it is tangential to the core issues in the case. By  
18 focusing all its relief on the software, the settlement buys into Ameritrade's mischaracterization  
19 of the security breach as a "spam issue."

20 Aside from the inadequacy of the proposed relief, three other features render it unfair to  
21 the class. First, the settlement provides for \$1.8 million in attorneys' fees, which, given the paltry  
22 nature of the class relief, makes counsel the primary beneficiary of the agreement. Second, it  
23 releases Ameritrade from a range of claims that were not even asserted in this case. Third, the  
24 class notice would further propagate Ameritrade's misleading characterizations of the breach by  
25 disclosing only the claims related to spam and by misrepresenting the terms of both Ameritrade's  
26 release from liability and the relief offered to the class.

27 Under these circumstances, the parties have not, and cannot, meet their burden of  
28 demonstrating that the proposed settlement is fair. Indeed, the settlement would provide even

1 less than the year of free credit monitoring and 50 free trades that Ameritrade *voluntarily* gave to  
2 clients who complained about the problem. Elvey Decl., Exh. 7. For these reasons, preliminary  
3 approval of the proposed settlement should be denied.

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

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

8 As proposed class counsel have conceded, the issue of stolen email addresses and  
9 resulting spam is only one aspect of this case. Pls.' Resp. at 6 ("Foremost, the Settlement  
10 addresses identity theft."); Tr. 10-11. In actuality, the scope of the data breach went far beyond  
11 email addresses, giving hackers unrestricted access for twenty-three months to the sensitive data  
12 of six million Ameritrade clients, including social security numbers, birth dates, account  
13 numbers, phone numbers, and addresses. Def.'s Resp., Exh. 1 at 1. This data includes the types  
14 of personal information (name, address, date of birth, and social security number) that are  
15 collectively known as a "full identity" and that are prized on the black market for their  
16 versatility. See Symantec Enterprise Security, *Symantec Global Internet Security Threat Report*,  
17 April 2008, at 17-19, 81, [http://eval.symantec.com/mktginfo/enterprise/white\\_papers/b-](http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiii_04-2008.en-us.pdf)  
18 [whitepaper\\_internet\\_security\\_threat\\_report\\_xiii\\_04-2008.en-us.pdf](http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiii_04-2008.en-us.pdf) ("Threat Report"). In the  
19 hands of a thief, a person's full identity can cause far more harm than an email address: "With a  
20 full identity, a criminal can easily obtain government issued documents, commit credit card  
21 fraud, open bank accounts, obtain credit, purchase and/or steal homes, or even evade arrest by  
22 masquerading as someone else." *Id.*<sup>1</sup>

23 The parties have attempted to direct attention away from the fact that social security  
24 numbers were exposed to the question whether Ameritrade's consultant, ID Analytics, has  
25 detected "organized misuse" of this data. However, the parties have made no effort to

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

1 demonstrate the reliability or scientific validity of the company's methodology, or even really to  
2 explain what that methodology is. *See, e.g.*, Tr. 13. Because the parties have kept the ID  
3 Analytics reports confidential, Tr. 39, there is no way for class members to effectively examine  
4 or rebut the company's conclusions. Moreover, the ID Analytics declaration submitted by  
5 Ameritrade does not justify the level of enthusiasm that the parties have expressed for it. The  
6 declaration states that the company "analyzed a subset of identity elements of consumers  
7 identified by TD Ameritrade," but does not identify the "subset" of information or the consumers  
8 identified. Cook Decl. ¶ 10. It concludes from this data only that "[w]ithin the ID Network, for  
9 this specific period and for this population of consumers, ID Analytics found no evidence of  
10 organized identity theft." *Id.* Unlike the parties, ID Analytics asserts no opinion, much less an  
11 opinion with a reasonable degree of scientific certainty, that its failure to find evidence of  
12 organized identity theft proves that identity theft has not or will not occur.<sup>2</sup>

13 On the other hand, the very fact that hackers had long-term access to a database  
14 containing such valuable forms of private data is a strong reason to believe that the data was in  
15 fact stolen. A person's "full identity," according to one recent report, sells for about \$1 to \$15 on  
16 the underground market. Threat Report at 12. Email addresses, alone, on the other hand, sell for  
17 \$.83 to \$10 per *megabyte*, meaning one full identity is likely worth more than thousands of email  
18 addresses combined. *Id.* Under these circumstances, Ameritrade's claim to have no evidence that  
19 social security numbers were taken is no different than if it had claimed, after watching armed  
20 robbers coming out of a bank carrying bulging sacks, to have "no evidence" that any money was  
21 stolen. The company's claim of ignorance is especially unimpressive given that Ameritrade said  
22  
23  
24

---

25  
26 <sup>2</sup> The conclusions of ID Analytics are somewhat beside the point, because class members are entitled  
27 to know if there is even a *risk* that hackers took their highly sensitive data so they can make up their  
28 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.

1 the same thing about email addresses for almost two years while its clients were providing it with  
2 exactly the evidence it claimed it did not have.<sup>3</sup>

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

5 In response to the data leak, the settlement agreement specifies that Ameritrade will  
6 perform two kinds of security tests—account seeding, which creates dummy accounts to help  
7 track down the source of a breach, and penetration tests, which simulate a hacker’s attempt to  
8 break into its system—and that it will employ ID Analytics to test for organized misuse of the  
9 data. Agmt. § IV(A)(2), (3), (5). The settlement also goes out of its way, however, to make clear  
10 that the company is already doing these things and would be doing them even in the absence of a  
11 settlement. The agreement provides that Ameritrade will “continue” the specified practices,  
12 noting particularly that account seeding is “currently is in place” and that it “has retained” ID  
13 Analytics, whose analyses “have already been performed.” *Id.* Indeed, as to ID Analytics, the  
14 settlement provides that Ameritrade must only finish out its *existing contract* with the company,  
15 something that, presumably, it is already obligated to do. *Id.* § IV(A)(5). The settlement does not  
16 require Ameritrade to adopt *any* new security measures to remedy the problems giving rise to the  
17 lawsuit, or even to reveal what those security problems were and how it has fixed them.

18 The settlement waters down these provisions even more by specifying that Ameritrade is  
19 obligated to continue doing what it is already doing for only a brief period of time. As for  
20 penetration tests, the company promises to conduct “bi-annual” testing, but only through  
21 December 31, 2009, giving it time for only one or two such tests. *Id.* § IV(A)(2). Account  
22 seeding is required to continue only through the end of 2008, but the settlement further provides  
23 that the company “may change the methodology as it deems appropriate, provided the new  
24 method is no less rigorous than the one that currently is in place.” *Id.* § IV(A)(3). Worst of all,  
25

26 <sup>3</sup> Around the time the breach became public, Elvey’s social security number was used to open an  
27 account and run up \$2500 in unauthorized charges. Elvey is careful with his personal information  
28 and knows of no other way the number could have been obtained.

1 Ameritrade promises to retain ID Analytics only through the end of September 2008, when its  
2 current contract with the company ends, a period that will almost certainly expire before class  
3 members are notified of the settlement. *Id.* § IV(A)(5). After these short periods expire,  
4 Ameritrade is free to return to whatever lax security policies it chooses, effectively eviscerating  
5 whatever value these security practices may have had. *See Schwartz v. Dallas Cowboys Football*  
6 *Club, Ltd.*, 157 F. Supp. 2d 561, 573 (E.D. Pa. 2001) (finding the value of settlement's injunctive  
7 relief to be "minimal at best" where it would remain in place for only 1-2 years).

8 In any case, the specified security measures are well below the minimum of what would  
9 be expected from any responsible financial services company. Elvey Decl. ¶ 21. To have any real  
10 impact on the security of client data, the settlement would have to provide for a set of best  
11 practices modeled on an existing industry standard. These practices would include, at least, a  
12 written security plan, a security audit to detect existing vulnerabilities, and periodic reassessment  
13 audits to ensure security is maintained. *Id.* ¶ 26. They would also include security controls such  
14 as encrypting and limiting access to high-risk data. *Id.* And finally, to get at one of the core  
15 problems giving rise to this case, a fair settlement would provide some way for clients to report  
16 security vulnerabilities so that they would be acted upon instead of ignored.

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

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

28

1 Proposed class counsel touts this system as one of the most important aspects of the  
2 settlement. Tr. 33-34. In actuality, it provides class members with nothing. Ameritrade has  
3 admitted that it would offer customer service to its clients even in the absence of the settlement  
4 agreement. Tr. 30-31. Indeed, Ameritrade's website reveals that it is *already* offering special  
5 customer service related to identity theft. The website states that the company has "a designated  
6 team responsible for reviewing potential threats to clients' assets and information," and advises  
7 those who suspect they may be victims of identity theft to call the company, where "Client  
8 Services representatives are trained to help you." See [http://www.tdameritrade.com/security/  
9 knowTheThreats/knowTheThreats.html](http://www.tdameritrade.com/security/knowTheThreats/knowTheThreats.html); [http://www.tdameritrade.com/security/  
10 knowTheThreats/securityIssue.html](http://www.tdameritrade.com/security/knowTheThreats/securityIssue.html). The remainder of the process is equally pointless.  
11 Ameritrade clients do not need the benefit of a settlement agreement to ask the company for  
12 compensation that it can grant or deny in its discretion, and, as the agreement makes clear, the  
13 option of submitting disputes to binding arbitration is already "provided in the customer  
14 agreement with the company." Agmt. § IV(A)(7)(d).

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

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

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

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

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

23 As plaintiffs convincingly argued in their motion for a preliminary injunction,  
24 Ameritrade’s failure to disclose the security breach, a fact relevant to the agency relationship  
25 between Ameritrade and its clients, violated the company’s fiduciary duty. The failure to  
26 disclose would also state a strong claim under the California Data Protection Act, Cal. Civ. Code  
27 § 1798.82, which provides that any company doing business in California must disclose security  
28 breaches after “discovery or notification of the breach in the security of the data to any resident

1 of California whose unencrypted personal information was, or is reasonably believed to have  
 2 been, acquired by an unauthorized person.” A nearly two-year delay in admitting the breach is  
 3 not made “in the most expedient time possible” as required by the Act. *Id.* Moreover,  
 4 Ameritrade’s claims that its servers were subject to a high level of security—at a time when it  
 5 was actually suffering an ongoing breach—was a misrepresentation about a material fact that  
 6 would have misled any reasonable consumer about the advisability of signing up for an  
 7 Ameritrade account, thus stating a claim under California’s Consumers Legal Remedies Act and  
 8 Unfair Competition Law.<sup>4</sup>

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

20 **B. The Required “Warning” on Ameritrade’s Website Is Not a Warning at All.**

21 Perhaps the most disturbing aspect of the proposed settlement is that it would waive all  
 22 the class’s claims regarding the security breach without requiring Ameritrade to provide proper  
 23 notice that the breach even occurred. The only aspect of the settlement that is even potentially  
 24 relevant to this problem is the requirement that Ameritrade place a so-called “warning” on its  
 25

26 <sup>4</sup> To be sure, it may be difficult to prove damages common to the class resulting from identity theft.  
 27 This fact, however, only increases the importance that the class receive injunctive relief. *See Walters*  
 28 *v. Reno*, 145 F.3d 1032, 1048 (9th Cir. 1998); *Gilder v. PGA Tour, Inc.*, 936 F.2d 417, 423 (9th Cir. 1991).

1 website. Agmt. § IV(A)(1). The language of the required statement, however, sounds more like  
2 general background information than an important warning to Ameritrade clients. *Id.* (“Go to  
3 Security Center for important information on protecting your assets from online threats such as  
4 identity theft, phishing, spyware, viruses, email fraud, and stock touting spam.”).

5 Moreover, the settlement includes no requirements regarding what clients will see when  
6 they click on the link, providing only that it will be “a warning to customers regarding stock  
7 spam.” *Id.* The agreement does not require that Ameritrade warn customers about the *particular*  
8 stock scams to which its clients have been subjected, that Ameritrade is responsible for leaking  
9 clients’ email addresses, or that their social security numbers have been exposed to hackers.  
10 General background information may be useful, but any general notice about stock spam that  
11 fails to mention that Ameritrade customers are at particular risk would, by omitting a material  
12 fact, be itself misleading.

13 Finally, the “warning” seems designed so that it will be read by as few class members as  
14 possible. The settlement provides that it be posted on Ameritrade’s website for “one week at a  
15 time, four times during a 12 month period,” requiring it to be put up and taken back down four  
16 times over the course of a year. *Id.* There is no legitimate basis for this provision—which  
17 actually requires more work by Ameritrade—other than to conceal the warning from Ameritrade  
18 clients.

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

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

2 Although spam is only one aspect of this case, it is the target of the only relief of any  
3 possible value: a one-year subscription to Trend Micro Internet Security Pro anti-spam software.  
4 The provision of this software does not render the settlement fair. The Court has a responsibility  
5 “to ensure that the settlement provides real value” by offering relief that the class will actually  
6 use. *Sylvester v. Cigna Corp.*, 369 F.Supp.2d 34, 49 (D. Me. 2005); *see also* 2003 Advisory  
7 Committee Notes, Fed. R. Civ. P. 23(h) (“Settlements involving nonmonetary provisions for  
8 class members also deserve careful scrutiny to ensure that these provisions have actual value to  
9 the class.”). Here, the settlement would leave many class members without any relief. The  
10 software will be worthless to the many class members who already have anti-spam software or  
11 who use popular online email clients like Gmail, Yahoo!, and Hotmail that are free of charge and  
12 have anti-spam capabilities built in. Moreover, many class members will have already changed  
13 their email addresses, either because they have been deluged with spam related to the data breach  
14 or for some other reason. Although the software will not be completely without value to these  
15 class members, they will no longer be able to use it for its intended purpose: to block the  
16 fraudulent spam caused by Ameritrade’s data breach. These class members will thus have little  
17 or no incentive to obtain the software.

18 Because the settlement requires class members to log into a website to download the  
19 software rather than requiring Ameritrade to mail it to them, the value of the settlement is further  
20 reduced. Experience has shown that recovery rates drop dramatically when class members are  
21 required to take additional steps to obtain their recovery. *See Buchet v. IIT Consumer Finance*  
22 *Corp.*, 845 F.Supp. 684, 693-96 (D. Minn.1994), *amended*, 858 F.Supp. 944 (discussing how the  
23 likely rate of coupon redemption affects the settlement’s value to the class). Downloading the  
24 software may be extremely inconvenient for those class members who lack a broadband Internet  
25 connection and are forced to spend hours downloading it over a phone line. Although the parties  
26 bear the burden of providing a valuation for the settlement on which a reasonableness  
27 determination can be based, they make no effort to determine what percentage of the class would  
28 likely download the software, making accurate valuation of the settlement impossible. *See In re*

1 *GM Corp. Pick-Up Truck*, 55 F.3d at 808 (settlement was not adequate, among other reasons,  
2 because use of supplied coupons during the redemption period would have been difficult).<sup>5</sup>

3 Even for those who do have a use for anti-spam software, the value of the relief is  
4 minimal. Counsel for both sides value the software at its retail price of \$69.95, but Trend Micro  
5 often provides rebates that, when combined with retailer discounts, push the price to \$0. *See*  
6 *Elvey Decl.*, Exh. 2 (April 2, 2008 Fry's advertisement offering Trend Micro free after rebate).  
7 The cost of the software to Ameritrade is itself very low, requiring Ameritrade to pay \$6 million  
8 for the right to distribute the software to its clients, or about \$1 for each of the approximately six  
9 million class members. That number may also be deceptive, however, because it appears that  
10 Ameritrade may have a preexisting relationship with Trend Micro that, although already  
11 established, it is now attempting to claim as a benefit of the settlement. According to the  
12 declaration of Trend Micro's sales manager, Ameritrade's \$6 million contract with the company  
13 allows it to distribute copies of the software between December 2007 and March 2011, meaning  
14 that Ameritrade *already has* a deal with Trend Micro that allows it to distribute software even  
15 before the settlement is finalized. *Thomas Decl.* ¶ 11. If Ameritrade is benefitting from this  
16 arrangement with Trend Micro, or if it would have entered into the contract regardless of the  
17 settlement, that would provide further reason to find that the settlement is not fair, adequate, or  
18 reasonable.

19 Finally, even setting aside its nominal value to some class members, the anti-spam  
20 software makes no sense as the primary relief for plaintiffs' claims because it includes no relief  
21 relevant to the core issues in the complaint. Although it was spam that originally drew Elvey's  
22 attention to the security breach, to direct all relief toward spam while ignoring the breach itself is  
23 to confuse the symptom with the disease. Without injunctive relief requiring improvements in  
24

---

25 <sup>5</sup> Redemption rates in class action cases are often 10% or less. *See, e.g., In re Compact Disc*  
26 *Minimum Advertised Price Antitrust Litig.*, 370 F.Supp.2d 320, 321 (D. Me. 2005) (2% submission  
27 rate); *Buchet*, 845 F.Supp. at 695 (rejecting settlement with 3% redemption rate); *Strong v. Bellsouth*  
28 *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).

1 Ameritrade's security practices or accurate notice to the class, the provision of the software does  
2 not make the settlement any more fair.

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

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

14 Because the parties have not provided any way to accurately judge the value of the in-  
15 kind relief to the class, it is impossible to determine the reasonableness of fees by reference to  
16 the value of the settlement. There are particular reasons, however, to be suspicious of the fees  
17 here. First, the provision of a fee to which the defendant has agreed creates the risk that class  
18 counsel may have bargained away valuable relief "in exchange for red carpet treatment on fees."  
19 *Weinberger v. Great N. Nekoosa Corp.*, 925 F.2d 518, 524-25 (1st Cir. 1991). Second, "the fact  
20 that the settlement involved non-cash relief only . . . is recognized as a prime indicator of suspect  
21 settlements." *In re GM Corp. Pick-Up Truck*, 55 F.3d at 80. And third, because the proposed  
22 attorneys' fees are not linked to how much relief is actually obtained by the class, there is no  
23 incentive for class counsel to ensure that the class obtains any relief with actual value. See *Polar*  
24 *Int'l Brokerage Group v. Reeve*, 187 F.R.D. 108, 119-20 (S.D.N.Y. 1999).

25 In this context, the \$1.8 million fee provided by the settlement is excessive in relation to  
26 the minimal value of the relief and the limited work performed. See *In re GM Corp. Pick-Up*  
27 *Truck*, 55 F.3d at 803 (holding fees excessive where "the settlement did not maximize the class  
28 members' interests"). This is especially true given that proposed class counsel limited its

1 discovery to a single deposition, relied primarily on evidence provided by Elvey, and took little  
2 risk in laying out total expenses of \$9000. *Id.* (“[C]lass counsel effected a settlement that would  
3 yield very substantial rewards to them after what, in comparison to the \$9.5 million fee, was little  
4 work.”); Agmt. § IX. Indeed, considering the size of the fee provided by the settlement, proposed  
5 class counsel’s insinuation that Elvey is objecting based on a vaguely alleged plan to garner  
6 publicity for his consulting business is ironic. On the contrary, Elvey’s opposition puts at risk the  
7 \$10,000 service award the proposed settlement would provide him. Amt. § XIII(A). In truth,  
8 Elvey may be the only one putting the class’s interest above his own.

9 Nor has counsel shown that its lodestar figure is reasonable. It is impossible to judge the  
10 fairness of the 1600 hours claimed by counsel given that they did not submit detailed time  
11 records. *See In re Washington Public Power Supply System Securities Litigation*, 19 F.3d 1291,  
12 1305-06 (9th Cir. 1994) (“The party petitioning for attorneys’ fees bears the burden of submitting  
13 detailed time records justifying the hours claimed to have been expended.”) (internal quotation  
14 omitted). For example, there is no way without detailed time records to determine whether  
15 certain hours were unnecessary, excessive, or duplicative. *Id.* (holding that hours may be reduced  
16 for these reasons).

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

18 The broad scope of the release, which waives the class’s right to bring claims that were  
19 not even asserted in this case, is another reason why the proposed settlement is unfair. The  
20 agreement specifies that the class waives all right to bring any class claims against Ameritrade  
21 that were or *could have* been brought in this case, except for individual claims for identity theft.  
22 This release is too broad because it is not limited to claims arising out of the subject matter of  
23 this case. Class members should not be required to waive their right to bring other actions against  
24 Ameritrade in order to settle their claims regarding this particular breach. *See Rossman &*  
25 *Edelman, Consumer Class Actions* § 12.3.3 (2006) at 165 (“Plaintiffs’ counsel should not allow

26 ///

27 ///

28 ///

1 any release phrased in vague terms, such as ‘all claims which could have been brought.’”). Class  
2 counsel did not purport to represent the class on these claims, and therefore cannot now release  
3 them. *See Nat’l Super Spuds v. N.Y. Merc. Exchange*, 660 F.2d 9, 18-20 (2d Cir. 1981).

4 Counsel for both sides stress that individual claims for identity theft are not released. But,  
5 assuming that by “identity theft” the parties are referring to claims for damages resulting from  
6 stolen personal information, the release would still abandon class members’ individual claims  
7 against Ameritrade for failing to notify them of the breach and for falsely advertising the security  
8 of its services. Moreover, even though the agreement specifies that individual *claims* for identity  
9 theft survive, it also provides what appears to be an exclusive *process* by which those claims  
10 must be resolved. Agmt § IV(A)(7). That process only becomes available if ID Analytics detects  
11 “organized misuse,” and, because ID Analytics has already said that no organized misuse was  
12 detected, the process by which claims are to be resolved would most likely never become  
13 available. *Id.* § IV(A)(6). Even if organized misuse *is* detected, the settlement provides for claims  
14 to be resolved through either Ameritrade’s customer service or binding arbitration. Thus, class  
15 members, even if retaining the right to seek relief for identity theft, give up the right to pursue  
16 that relief in court.<sup>6</sup>

17 **VI. The Defective Class Notice Provides an Independent Reason to Reject the**  
18 **Settlement.**

19 **A. The Notice Would Further Deceive Class Members by Misrepresenting the**  
20 **Nature of the Claims and Relief.**

21 Due process requires that absent class members receive notice of material terms of class  
22 settlements. *Mullane v. Cent. Hanover Bank & Trust Co.*, 339 U.S. 306, 313 (1950). Far from  
23 providing such notice, the settlement here perpetuates Ameritrade’s misrepresentation of the data  
24 breach as a “spam issue,” leaving class members in the dark about what claims they are asserting  
25 and giving away. The notice describes the complaint as “alleg[ing] that an unauthorized third

26 \_\_\_\_\_  
27 <sup>6</sup> It is possible that the parties intended the process provided in the settlement agreement to be only  
28 an alternative to a suit in court. If so, the agreement should be clarified to ensure that class members  
are not unknowingly subjecting themselves to binding arbitration.

1 party acquired e-mail addresses of the Company's accountholders that were then used by  
2 spammers to send unsolicited commercial emails promoting certain stocks." There is no mention  
3 of the other claims in the complaint, including the allegations that social security numbers and  
4 other sensitive data were also exposed. Nor does the notice mention that the class is asserting  
5 claims for breach of fiduciary duty and unfair competition, or that the class is releasing these  
6 claims along with any other claims that *could have* been brought in the litigation. These  
7 characterizations are particularly misleading because, by treating the case as one about spam, the  
8 notice makes the only real relief in the case—the anti-spam software—appear much more  
9 reasonable than it actually is.<sup>7</sup>

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

20 Finally, by omitting the amount of attorneys' fees, the summary notice conceals the fact  
21 that the only cash benefit provided by the settlement is the \$1.8 million awarded to proposed  
22 class counsel. Without a "clear estimate of attorneys' fees and expenses," class members are thus  
23 unable to "determine the possible influence of attorneys' fees on the settlement in considering  
24 whether to object to it." *See In re Gen'l Motors Corp. Engine Interchange Litig.*, 594 F.2d 1106,  
25

26 <sup>7</sup> The notice also continues to downplay the extent of the breach by repeating, in bold letters,  
27 Ameritrade's misleading claim that there is "no evidence of organized misuse of personal  
28 information."

1 1130-31 (7th Cir. 1979); *see also* *Staton*, 327 F.3d at 963 n.15; *Piambino v. Bailey*, 610 F.2d  
2 1306, 1328 (5th Cir. 1980). There is no reason why it would have been difficult to include the  
3 amount of fees in the summary notice. The notice already states that “provisions for attorneys’  
4 fees . . . are set forth in the complete notice,” which takes up about as much space as actually  
5 disclosing the number would have.

6 **B. The Notice Is Poorly Designed to Reach Class Members or to Allow Them to**  
7 **Opt Out.**

8 The proposed settlement provides that the class notice will be delivered only by email  
9 except in cases where Ameritrade does not have a class member’s email address. Under the  
10 circumstances here, however, email would be a particularly poor way to notify the class. The  
11 security breach that is the subject of the class’s claims caused class members to receive large  
12 quantities of spam, prompting class members to stop checking the email accounts they had  
13 supplied to Ameritrade. *See* Elvey Decl. ¶ 25; Sweet Decl. ¶ 7; Winzig Decl. ¶ 10. Even those  
14 who still check their accounts may miss the email under the deluge of Ameritrade-related spam.  
15 This is especially likely because the proposed settlement includes no details about how the email  
16 will be delivered, such as the email’s subject line, the size of the font, and whether the notice will  
17 be included in the body of the email or as an attachment. Given Ameritrade’s history of burying  
18 any mention of its security breach, it would not be surprising to see an email that looks like one  
19 of many informational or promotional emails that Ameritrade routinely sends to its members and  
20 that are usually deleted without being read.<sup>8</sup>

21  
22  
23  
24  
25 <sup>8</sup> While allowing Ameritrade to email the notice to class members, the proposed settlement requires  
26 class members who wish to opt out to mail a total of three copies of the opt-out notice—one to the  
27 claims administrator and one each to the parties’ counsel. This requirement is totally unnecessary  
28 and seems designed for no purpose other than to make it difficult and burdensome for class members  
to exercise their opt-out rights.

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

3 The right of class members to be heard on the fairness and adequacy of a settlement  
4 includes an opportunity to develop the record supporting their objections, so that the settlement's  
5 adequacy can be tested through an appropriate, adversary process. *Girsh v. Jepson*, 521 F.2d 153,  
6 157 (3d Cir. 1975). Here, Ameritrade has kept most aspects of the breach secret and has refused  
7 the request of undersigned counsel to view the only discovery in the case—the single deposition  
8 of Ameritrade's security chief. The lack of any information about the breach other than  
9 Ameritrade's self-serving assertions prevents Elvey and other class members from evaluating  
10 key aspects of the case that bear on their decision whether to settle. To give Elvey and other class  
11 members the opportunity to challenge the propriety of the settlement, the Court should deny  
12 preliminary approval and order the parties to file in the public record all information necessary to  
13 evaluate the settlement's fairness. This would include, at least, the record of the deposition, the  
14 reports by ID Analytics, any contracts with Trend Micro, and any other evidence on which the  
15 parties intend to rely. Making the evidence public will ensure that some class members will not  
16 have preferential access to it while others, who have an equal interest in the material, are left in  
17 the dark. As the U.S. Court of Appeals for the Fifth Circuit recently observed, a process in which  
18 class members are "deprived of information necessary to contest" a settlement because critical  
19 information is kept secret is "inherently flawed." *In re High Sulfur Content Gasoline Prods.*  
20 *Liab. Litig.*, 517 F.3d 220, 232 (5th Cir. 2008).

21 **VIII. Elvey's Signature on the Settlement Agreement Should Not Affect this Court's**  
22 **Analysis of His Objections.**

23 Counsel may argue that the Court should not consider Elvey's arguments because he  
24 already assented to the terms of the settlement agreement. Whether Elvey's name appears on the  
25 agreement, however, is irrelevant. To begin with, the agreement is not final or enforceable until  
26 it has obtained the approval of this Court, and Elvey made his opposition known to the Court in  
27 time for it to be considered at the hearing on preliminary approval. Moreover, as a single  
28 member of a proposed class, Elvey has no authority to bind the remainder of the class (nor, as a

1 candidate for representation of a class that has not yet been certified, does proposed class  
2 counsel). Indeed, as the accompanying declarations demonstrate, Elvey is not the only class  
3 member dissatisfied with the settlement. *See* Sweet Decl. ¶ 7; Winzig Decl. ¶ 9; *see also, e.g.,*  
4 Paul McNamara, *Judge Halts Ameritrade Settlement that Would Mean a Boon for Lawyers, a*  
5 *Pittance for Victims*, Network World, June 16, 2008 (class member describing the proposed  
6 settlement as a “warm bucket of spit”) (Elvey Decl. Exh. 5). The Court has a duty to protect the  
7 interests of absent class members regardless of whether particular class representatives have  
8 assented to its terms. *See Grant v. Bethlehem Steel Corp.*, 823 F.2d 20, 23 (2d Cir. 1987).<sup>9</sup>

9 Although Elvey was ultimately persuaded to add his name to the agreement, his former  
10 counsel cannot claim to have been surprised by his opposition. Since the beginning of the  
11 litigation, Elvey had repeatedly expressed his views on what components he thought should be  
12 included in a fair settlement, but none of those components was included in the settlement that  
13 was presented to him as the final, unchangeable version of the agreement. *Id.* ¶ 15. When Elvey  
14 hesitated to accept this agreement, he was told that, unless he consented, he would be removed as  
15 class representative and the settlement would proceed to approval without him. *Id.* ¶ 19.  
16 Proposed class counsel’s objection to Elvey’s position therefore arises not so much from Elvey’s  
17 strong disagreement with the settlement’s terms—of which they were well aware—but from the  
18 fact that he had the temerity to express those views to the Court.<sup>10</sup>

19 Proposed class counsel’s memorandum also includes various other meritless personal  
20 attacks against Elvey that are irrelevant to the fairness of the settlement. Elvey will not respond  
21 to them here, other than to say that most of the complaints arise from the fact that he was

---

22  
23 <sup>9</sup> Elvey never actually agreed to the full settlement, because the version he signed lacked the  
24 proposed class notice forms, which are a material element of the agreement and, as detailed in  
section VI, one of the reasons for Elvey’s opposition to it.

25 <sup>10</sup> The threat to remove Elvey as class representative was the threat to which Elvey referred at the  
26 hearing on preliminary approval. Elvey Decl. ¶ 19. Elvey did not have the opportunity to elaborate  
27 on his statement and never implied that he was threatened with physical harm. Nevertheless, the  
28 threat to remove him as class representative was a serious one given that it meant he would lose the  
\$10,000 guaranteed to him by the agreement. *Id.* Elvey also feared that if the settlement proceeded  
without him, he would be unable to fulfill his fiduciary duty to protect the interests of the class. *Id.*

1 proceeding effectively as an unrepresented party and was attempting, against the interests of his  
2 own counsel, to make his opposition to the settlement known.

3 **CONCLUSION**

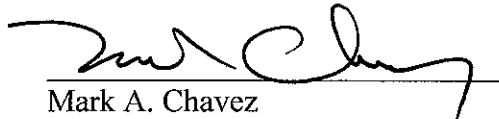
4 For the foregoing reasons, this Court should refuse to grant preliminary approval to the  
5 proposed settlement and should order the parties to file and serve on Elvey's counsel the  
6 transcript of the deposition that occurred in this case and any other evidence on which the parties  
7 have relied or intend to rely in support of the settlement's fairness.

8  
9 Date: September 9, 2008

Respectfully submitted,

10 CHAVEZ & GERTLER, LLP

11 PUBLIC CITIZEN LITIGATION GROUP

12  
13   
14 \_\_\_\_\_  
Mark A. Chavez

15 Attorneys for Plaintiff