Yale Symposium on Law and Technology

Spring 2001

Online Securities Trading: Triggering the Cycle of Technological Innovation and Congressional Response

Jordan Silber[†]

Cite as: 4 YALE SYMP. L. & TECH. 5 (2001)
<http://lawtech.law.yale.edu/symposium/s01/note_silber.htm>

I. INTRODUCTION

¶1 The introduction in the late 1990s of Internet securities trading (hereinafter "Cybertrading," as opposed to "Traditional Trading") is the most significant technological advance in the area of consumer financial services in the last twenty years.[1] This Note proposes that in light of the development of Cybertrading, new consumer protection legislation may be warranted. The evidence presented here will show that many of the same risks and policy considerations which led Congress to enact consumer protection legislation with respect to credit cards, ATM cards, and Traditional Trading are similar or identical to the risks and policy considerations associated with Cybertrading. If such prior measures may be fairly characterized as successful, similar steps by Congress to protect Cybertraders may be in order.

¶2 Historically, Congress has passed consumer protection legislation subsequent to the emergence of new financial services technologies. This trend started in the late 1960s, when the securities brokerage industry was faced with a crisis: the physical exchange of paper share certificates, required for every transaction, had placed an enormous administrative burden on issuers and brokers.[2] To accommodate the rapidly expanding volume of trades, technology was utilized to create clearing corporations which held the physical certificates and recorded transactions on their own books, thereby eliminating the requirement that physical share certificates be exchanged for each individual transaction.[3] By employing this new technology, the securities industry was able to handle a volume of trading previously considered impossible.[4]

¶3 With this new technology came new problems. Since individual investors no longer possessed their own share certificates, they were subjected to various new risks: errors might be made in calculating their ownership, and the business entities responsible in trust for their individual interests might engage in fraud or become insolvent, creating a risk of monetary loss.[5] The additional risks, and the lack of rules with which to control them, led Congress to enact investor-oriented legislation. The most important consumer protection development was the enactment in 1970 of the Securities Investor Protection Act ("SIPA"), designed to protect consumers from loss due to fraud and insolvency.[6]

¶4 The securities industry was not the lone financial services industry regulated in accordance with Congress' desire to protect consumers from losses attributable to new technology.[7] The introduction of the credit card and, later, the ATM card, led Congress to enact statutes designed to protect the users of these products from financial losses associated with their use.[8]

¶5 This Note proposes that the stage is set, once again, for the introduction of consumer protection legislation. Part II describes the various vulnerabilities faced by Cybertraders today, and examines whether brokers or traders are better positioned to mitigate the risk associated with each vulnerability. Part III outlines steps Congress has taken in the past to protect users of credit cards, ATM cards, and Traditional Trading services, and explores whether those measures have achieved their intended results. Part IV explains why the remedy currently available to Cybertraders, industry-sponsored arbitration, is insufficient as a means of protection. Part V concludes that prior protections have been successful, and goes on to suggest model legislation designed to balance Cybertrader protection against the needs of the brokerage industry.

II. Vulnerabilities Faced By Cybertraders

¶6 An examination of pending class action lawsuits and arbitration proceedings (as reported in the quarterly SEC filings of the major Cyberbrokerages[10] and in press releases[11]) suggests that, to date, five types of vulnerabilities have given rise to claims by Cybertraders against Cyberbrokerages. These five categories are: (1) claims for difficulty of access or complete interruption of service, including interruptions due to denial of service attacks by hackers;[12](2) other losses caused by hackers, such as unauthorized trading or withdrawal;[13] (3) trades executed or not executed due to errors attributable to the Cyberbroker's software;[14] (4) losses due to reliance by Cybertraders on erroneous information provided by the Cyberbrokerage;[15] and (5) failure to mitigate damages due to the Cyberbroker's lack of response or untimely response to reported problems.[16]

¶7 SEC quarterly reports[17] for the ten leading Cyberbrokerages,[18] indicate that seven of the top ten Cyberbrokerages are currently facing class action suits related to losses incurred by Cybertraders. E*Trade alone has five class actions pending, as reported in their 10-Q/A filing of June 30, 2000.[19] In addition to the class actions, there are numerous single-investor arbitrations, as evidenced by a news release search,[20] commentary from the chairman of the Securities and Exchange Commission,[21] and the emergence of boutique law firms that deal exclusively in representing investors at arbitrations.[22]

¶8 Vulnerabilities have arisen because the technology is new and often untested.[23] Cyberbrokerages are expanding at unprecedented rates and are often unable to ramp up technology services proportional to customer demand.[24] In addition, Cyberbrokerages are often forced to respond defensively to attacks on their technology that they were unable to anticipate.[25] While Cyberbrokers' efforts might mitigate these vulnerabilities, some level of vulnerability simply inheres in the use of the new technology.

¶9 As new business entities operating in a tight labor market, Cyberbrokerages are often short-staffed and lack qualified personnel.[26] Therefore, Cyberbrokerages are often unable to respond to vulnerabilities in a timely fashion; recently it took E*Trade nine months to close a serious security gap called "cross site scripting" which, if exploited, would have allowed hackers to access and trade on users' accounts.[27] Whether caused by labor shortages or otherwise, poor response time can increase losses when Cyberbrokers fail to act to mitigate damages,[28] and deserves consideration as its own category of vulnerability.

¶10 In fact, each of the five identified types of vulnerabilities deserves separate consideration inasmuch as each arises from distinct technological considerations, illuminates different policy concerns, and requires a different statutory solution.

A. *Claims for difficulty of access or complete interruption of service*

¶11 These claims comprise the majority of pending class actions against Cyberbrokers. For example, every one of the five pending class actions listed in E*Trade's most recent 10-Q/A alleges either (1) total interruption of service,[29] (2) difficulty of access, where access was eventually possible but Cybertraders allege that the slow response time led to undue losses,[30] or (3) difficulty of access from a particular geographic area.[31] Claims arising from losses due to access and interruption issues are also pursued in individual arbitration actions. Approximately ninety percent of pending actions relate to these types of claims.[32]

¶12 These claims, whether made individually or on behalf of a class, typically state causes of action based on fraud, deceit, negligent misrepresentation, unjust enrichment, and, where available, statutory claims for unfair business practices.[33] The complaint in the *Cooper v. E*Trade* class action is typical.[34] Plaintiffs allege that due to the explosive growth of both users and transactions, Cyberbrokerages are unable to handle the volume of transactions "reasonably" quickly.[35] Furthermore, some Cyberbrokers, including E*Trade, have allegedly continued aggressive marketing campaigns resulting in an increase in the number of users and transactions, thereby causing further diminution in service.[36] Other Cyberbrokers, including T.D. Waterhouse, stopped or reduced advertising due to technical difficulties.[37]

¶13 Besides claiming that services are "unreasonably" slow, plaintiffs often allege that the service is slower than has been promised in advertising.[38] For example, E*Trade advertisements tout that its Cybertrading system provides "rapid and high quality executions," executes market orders during market hours "within a matter of seconds," uses "state-of-the-art technology," and "allows trades 24-hours-a-day, from anywhere…in less than a minute."[39] In *Cooper*, plaintiffs allege that some market orders have taken more than twenty minutes to execute, that at times during market hours a user cannot log on to the system at all, and that even when a user can connect, it usually takes more than "a matter of seconds" to trade.[40]

¶14 Access and interruption problems occur either due to software and hardware failures, or to usage demands which exceed system capacity.[41] Exceptional usage demands occur in two cases: first, when hackers initiate denial-of-service attacks (designed to cripple systems by sending vast quantities of information to the Cyberbrokers' servers),[42] and second, when Cybertraders themselves place heavy demands on the brokers' systems.[43]

¶15 Problems appear to be worst when overall market volume is heavy, such as during a heated sell-off or rally.[44] As recently as 1997, E*Trade's Cybertrading system reportedly could handle only 7% of its users simultaneously.[45] During a period of heavy market activity, system capacity may be insufficient to satisfy demand, leading to access and trade execution problems.[46] This was the case on October 27 and 28, 1997, when the New York Stock Exchange fell 550 points on the first day and rose 330 points on the second, on record volume.[47]

¶16 Though E*Trade has been criticized as the most susceptible to system interruptions,[48] most of the major Cyberbrokers (including Charles Schwab[49] and National Discount Brokers[50]) have experienced system outages and service interruptions due to software and hardware problems, denial-of-service attacks, or both.

¶17 Evidence suggests that system overloads, whether caused by legitimate users or hackers, are related to the individual Cybertraders' software and hardware systems, as opposed to heavy Internet activity generally.[51] This is important, because it suggests that the ability to control satisfactory access lies in the hands of the individual Cyberbrokerages.

B. *Losses caused by hackers*

¶18 While hackers have caused problems other than denial-of-service attacks, detailed below, these other activities have not yet led to major litigation or arbitration.[52] For the most part, Cyberbrokers have been willing to indemnify users and absorb losses caused by hacking activity (other than denial-of-service attacks). For example, when hackers absconded with the account numbers of one percent of Fidelity users in 1998 and used the numbers to create debit cards for these accounts, Fidelity agreed to reimburse users for the losses without an arbitration demand.[53]

¶19 Hackers use a variety of schemes to cripple systems or fraudulently obtain data. These schemes have ranged from setting up bogus "look-alike" web pages and changing the DNS name server settings to direct clients of that Cyberbrokerage to the bogus page, where the traders unknowingly submit their usernames and passwords to the hackers,[54] to technical hijacking of entire username and password lists, followed by attempts to blackmail the Cyberbroker into paying ransom to prevent publication of the information.[55]

¶20 To date, apparently hackers have not gained unauthorized access to Cyberbrokers' accounts and placed bogus trades.[56] However, industry security experts warn that the worst may be yet to come, as hackers are highly skilled.[57] By 2010, the Justice Department estimates that 70% of all criminals will be computer literate.[58] And, not all attacks by hackers may be noticed; the FBI reports that 95% of hacker attacks go undetected.[59] Based on these trends, experts predict that the number of hacking incidents will increase in the future.[60]

¶21 One way in which Cyberbrokerages can combat hacking is to pursue advances in software – an effort some Cyberbrokers, including National Discount Brokers, admit warrants more attention.[61] Less obviously, however, Cyberbrokerages can also limit hacking by paying closer attention to who they hire.[62] Thomas Beach, a Senior Vice President at Fidelity, claims that only 27% of hacker incidents at Cyberbrokerages are caused by individual hackers; instead, the majority are caused by employees.[63] Recently introduced insurance products now allow Cyberbrokers to insure against hacker attacks, both for service interruptions, by way of business interruption coverage, and for casualty losses arising from theft of information or fraud.[64] While it may not be possible for Cyberbrokers to completely eliminate hacking incidents, Cyberbrokers possess the ability to curb losses due to hacking, by improving hiring processes and security systems, and tailoring insurance coverage.

C. *Trade execution errors attributable to the Cyberbroker's software*

¶22 Some losses due to software error fall within previously discussed categories of vulnerability, as such errors can cause system outages[65] or open the door to hackers.[66] However, problems with software also lead to more specific losses when errors occur during trade execution. Complaints by E*Trade customers Ali Khadavi and William Badgerow are typical of a line of claims asserted against the Cyberbrokers.[67] In the *Khadavi* arbitration, E*Trade stipulated that a software error caused an order to execute forty minutes after cancellation by the trader, who was awarded compensatory damages in excess of $61,000.[68] Meanwhile, the *Badgerow* arbitrators found that a software error had caused a sell order to be executed twice, resulting in a short position in the trader's account. Mr. Badgerow was forced to cover the position days later, at a cost of $23,000, which is the amount arbitrators awarded to the Cybertrader plaintiff.[69]

¶23 A distinguishing factor associated with these types of losses is that they are easily quantifiable. For example, when a trade is erroneously executed twice, the measure of damages is the difference between the purchase price of the second block of shares and the market price of the block at the time the trade is discovered and reversed by the brokerage. The ease with which these damages are fixed stands in contradistinction to claims for service interruption and outages. Damages from hacking may fall into either category, that is, they may be certain (as where a hacker withdraws a certain sum from an account), or uncertain (as where a hacker precludes a Cybertrader from accessing her account for some period of time).

¶24 Again, control lies within the hands of the Cyberbrokerage, which has the capacity to correct glitches with current systems, and to develop or procure more advanced systems should they be needed or become available.

D. *Reliance by Cybertraders on erroneous information provided by the Cyberbrokerage*

¶25 Reliance losses can be divided into three types, depending on the type of information conveyed in error: (1) misstatement of the price of a security; (2) misstatement of the balance of an account; or

(3) erroneous delivery of or failure to deliver trade confirmations, causing execution of additional trades or lack thereof.[70]

¶26 Failure to state the correct price of a security may arise simply due to posting the wrong price,[71] or, when the market value of a security posted simultaneously with the placement of a market order is not the timely price, causing the order to execute at a substantially different price than the price at which the Cybertrader is led to believe it will execute.[72]

¶27 Misstating the account balance may lead the Cybertrader to make trades which, when all is discovered, short the account, causing the Cybertrader to become indebted to the Cyberbroker, thereby incurring fees and interest. Alternatively, the trader may fail to make trades to close out positions due to a mistaken belief that the position is doing better than it actually is.[73] A final problem arises when confirmations are delivered in error, or not delivered at all. For example, in *Cooper*, the Cybertrader relied on the fact that confirmations were consistently sent; when one was not received, the trader believed the order had not been processed and placed the order a second time, leading to a loss.[74]

¶28 Sometimes, damages in these reliance actions are easily set (as where the user has proof of a misstated price, and the incorrect price can be adjusted), but at other times the task of fixing damages is not as clear (as where a Cybertrader claims she *would have* made a purchase had she had correct price information, leading to uncertainty regarding the legitimacy of her claim to lost profits). As reliance issues are caused by software, the ability to control or eliminate such reliance problems rests in the hands of the Cyberbrokerages.

E. *Failure by Cyberbrokers to mitigate damages*

¶29 Errors often lead to Cybertraders owning equities they should not own. The causes span the vulnerabilities heretofore discussed, such as an order being placed twice due to software error, or a hacker's denial-of-service attack preventing a trader from liquidating a position in a falling market, or incorrectly posted data causing a Cybertrader to execute a trade she would not have executed had the real price information been known. When these errors happen, the Cyberbroker's ability to limit damages depends on how quickly it receives information regarding the error, and whether it takes corrective action. In some cases, whole claims have been established, and in others, damages have been amplified based on the failure of Cyberbrokers to reasonably mitigate.[75]

¶30 Poor response time is only one factor. At times, Cyberbrokers decide wrongly that no corrective action is necessary, and by the time damages are fixed at arbitration, they have escalated.[76] This problem is exacerbated by the fact that Cyberbrokers are short-staffed, and lack senior level employees with adequate training to make these decisions.[77] In one case, E*Trade took five days to initiate a trade inquiry, forty days to conduct its investigation, and then decided to take no corrective action; the arbitrator decided corrective action was warranted.[78]

¶31 Cyberbrokers control the mechanisms available to access their personnel (by Internet, telephone, mail, in person or otherwise). They control the response time and quality of personnel dealing with Cybertrader inquiries. They control the mitigatory decisions made. Therefore, it is the Cyberbroker who is best able to minimize risk.

III. Past Congressional Action to Protect Consumers Using Traditional Trading Services, Credit Cards, and ATM Cards

¶32 With the introduction of clearinghouse technology for Traditional Trading, and later when credit card and ATM technologies were introduced, Congress acted to protect users from the risks associated with these new technologies.[79] The stated purpose of these technology-induced statutes, as well as the nature of each technology, its effects on consumers, and the political atmosphere in which each of the consumer protection statutes was enacted, put Cybertraders in a position which is similar to that of users of clearinghouse-based trading systems, and credit card and ATM patrons, just prior to the passage of protective legislation.

A. *Traditional Trading Services – The Securities Investor Protection Act of 1970 ("SIPA")*

¶33 SIPA was designed to protect customers of brokers, up to a certain dollar limit, from losses due to financial failure of the broker,[80] as well as from fraud.[81] Protective legislation was introduced in response to two factors: (1) the introduction of clearinghouse technology, designed to circumvent the need to provide individual paper shares to stockholders, and (2) market declines of the late 1960s, which led to the financial instability of brokers.[82]

¶34 Congress acted out of fear that absent paper shares, traders would be threatened in the event of a technical failure at a clearinghouse, or if the ownership of their shares was challenged.[83] Therefore, it was the new technology itself, the fact that the clearinghouse would take the place of the physical document, that led in part to the passage of the protective legislation. Similarly, Cybertrading is a new technology that has introduced certain risks to securities trading which are *inherent* risks associated with mere use of the technology itself. While SIPA adequately addressed the problems introduced by the clearinghouse, SIPA is inadequate as a means of protecting Cybertraders. To understand why this is the case, it is important to understand exactly how SIPA operates.

¶35 SIPA was introduced during a period in which many brokers were financially unstable, and was designed primarily to protect consumers from losses incurred during financial failure of their broker.[84] If a broker becomes insolvent, SIPA provides a mechanism by which the assets held by that broker may be transferred to a different, financially sound broker.[85] If there are not sufficient assets remaining to restore the trader's account to the proper level, SIPA will fund the repurchase of the requisite securities, and transfer them to the new broker.[86] While SIPA provides for very limited protection against unauthorized transactions, this protection only becomes effective if the liquidation process commences.[87]

¶36 Since SIPA does not otherwise provide for fraud protection, and because SIPA is targeted at curbing losses which traders might incur when their broker becomes insolvent, SIPA does not properly address the unique vulnerabilities which can arise in Cybertrading. Protective legislation to protect Cybertraders must specifically address the risks which arise from online securities trading.

B. *Credit Cards – The Truth In Lending Act ("TILA")*

¶37 The purpose of TILA was to "protect the consumer against inaccurate and unfair…credit card practices."[88] Congress decided to impose a maximum liability for credit card fraud perpetrated upon a consumer, in almost all situations, of $50.[89] The goal was to create a fair allocation of risk between the consumer and the financial institution; it was feared that if the consumer had zero liability for misuse, she would have little incentive to report loss or theft of the card.[90]

¶38 Throughout its existence, one justification for TILA has been that financial institutions, as for-profit business entities, make business decisions that are not always aligned with consumers' best interests. Therefore, it is argued that consumer protection legislation is necessary to protect consumers who might otherwise suffer undue financial losses from utilization of the new technology.[91] This argument suggests that financial institutions that want to make use of new technology should internalize the cost of doing so. If market conditions allow the institution to recover this cost from consumers as a whole, it may do so in the form of service fees or other charges spread across the user base. If it is unable to recover the costs, it will earn lower returns. At the point when the value added by the new technology is outweighed by its variable costs, the institution will either stop using the technology or invest in making it profitable. Either way, institutions are encouraged to utilize technology profitably, and no individual consumer is burdened with a huge personal loss.

¶39 This concept may be applied to Cybertrading, which—like credit card use—is a financial services technology that can result in substantial monetary losses for individual users. Therefore Cybertrading is a candidate for risk-allocation legislation.

C. *ATM Cards – The Electronic Funds Transfer Act ("EFTA")*

¶40 When ATM machines were introduced, demand for the new technology was explosive. Banks did not anticipate it, and they were unprepared to handle technical difficulties that arose during these systems' infancy.[92] As with Cybertrading, it was the service provider, and not the consumers, who could make systems more secure, and take other actions to reduce consumers' losses.[93] Just as state attorneys general stepped in to investigate ATM liability prior to the enactment of protective legislation,[94] so too has an attorney general intervened to investigate Cybertrading liability.[95] The technical and political factors which led to the passage of protective legislation for ATM users are similar to those which Cybertraders face today.

¶41 Several years after the introduction of ATM technology, Congress enacted EFTA for the primary purpose of providing individual consumer rights.[96] As with Traditional Trading, Congress was concerned that consumers be protected from risks that are inherent in the new technology. It wanted to spread the cost of protection to all consumers by forcing banks to internalize the cost of losses, rather than make users suffer potentially large individual losses.[97] Congress once again utilized the allocation of risk concept established in TILA, by imposing (in most cases) a $500 maximum loss on a consumer in the event that an ATM fraud is perpetrated against her.[98] EFTA, like TILA, denies protection if the consumer waits too long to notify the financial institution of loss or theft.[99] EFTA demands that the card user act reasonably, and when her behavior is unreasonable, she is expected to share in any loss that arises. EFTA lends additional support to the concept of avoiding individually devastating losses by way of a risk-allocation approach.

¶42 It is worth noting that the use of banking services and credit cards on the Internet have not created the need for new consumer protection legislation, as TILA and EFTA have proven to be sufficient for allocating risk. The liability provisions set forth in these statutes have been acceptable to card issuers, who, in striving to increase the usage of their cards,[100] have advertised current liability limits imposed by the statutes, or in some cases have voluntarily offered consumers a better deal.[101] TILA and EFTA are designed to allocate risk as to electronic systems, and are thus easily applied to the Internet framework. Because SIPA addresses Traditional Trading, no existing legislation suitably protects Cybertraders.

IV. Industry-Sponsored Arbitration is Insufficient as a Means of Consumer Protection

¶43 Most brokerage agreements between Cybertraders and their Cyberbrokerages contain arbitration agreements.[102] The Supreme Court has generally found these agreements to be enforceable,[103] though attempts to set them aside as contracts of adhesion have sometimes been effective.[104] Still, the large majority of Cybertraders' disputes end up in arbitration.[105] Approximately ninety percent of these claims are heard by the arbitration panels at the National Association of Securities Dealers ("NASD"), a broker-sponsored entity.[106] Arbitration panels at NASD are comprised of three members, at least one of whom must be an industry employee.[107] Despite the inclusion of brokers' employees on these panels, investors prevail in 62% of arbitrations at NASD, up from 47% in 1994,[108] and plaintiffs' lawyers acknowledge that an overhaul of the NASD arbitration process has generally yielded fairer hearings.[109] Thus the NASD appears to be a fair venue for Cybertraders.

¶44 Nevertheless, there are four reasons why arbitration is not a viable means of consumer protection for Cybertraders. First, the NASD system takes fifteen months to bring the average claim from filing to decision.[110] Second, a significant volume increase may strain the NASD's ability to adequately conduct arbitrations in the near future. Third, the NASD arbitration process is so complicated that, even in its "under-$25,000-claim 'easy filing system,'" the parties require representation by attorneys.[111] Fourth, the methods of proof are complex, requiring extensive discovery.[112] The net effect is that many consumers are either deterred from entering arbitration, or are required to expend substantial time, effort, and money to be made whole. While this is an inherent feature of litigation, there is a benefit to creating a simple statutory system to protect consumers using financial product technologies. A statutory scheme forces service providers to internalize costs, which provides incentive for them to eliminate deficiencies in the technology system—improvement solely within their power.

¶45 Consumers benefit from the broker's internalization of cost of risk in three ways. First, because of the incentive for brokers to minimize overall losses by improving the technology, consumers benefit from a better product. Second, consumers benefit by not being individually subjected to large losses. Third, as financial technology products are made safer, more consumers will utilize these products, and the costs of technical improvement will be spread across a larger user base, lowering the overall cost per user.[113] While having brokers absorb the occasional arbitration award provides some incentive for them to improve their services, forcing them to internalize the cost of technology-specific loss creates positive incentives that benefit both the broker[114] and the trader in the long run. I will call this process – the internalization of the cost of technology risk, followed by technical improvement, more usership, and, ultimately, a lower cost per user—the "Cycle of Improvement." While some providers might voluntarily internalize the costs discussed herein, or seek out and introduce safer technologies in order to gain a competitive advantage, this is an insufficient solution where the goal is to minimize individual losses and make systems safe for *all* users.

¶46 If safer products and heightened levels of protection are a valid measurement of success in protecting consumers, then it is reasonable to declare as successful the statutory solutions introduced with respect to previous consumer financial technologies. Credit cards now employ holograms, a safety feature offering greater security against fraud.[115] The vast majority of credit card and ATM card issuers offer easy, fast, round-the-clock access methods to report lost and stolen cards, thereby mitigating losses due to fraud. In short, having the technology providers internalize vulnerability losses has led to new protective measures. These measures have resulted in a reduction in per-user fraud loss. Furthermore, card issuers have increased their user base, leading to greater profits even with the cost of implementing the technological improvements.[116] In these cases, the Cycle of Improvement worked.

V. The Statutory Solution

¶47 Having defined the vulnerabilities to which traders are subjected when they use Cybertrading technology, and having looked at ways Congress has successfully addressed similar vulnerabilities in the past, I conclude that the present remedy—arbitration—is an insufficient protective mechanism for Cybertraders. Congress should once again adopt consumer protection legislation.

¶48 A statutory solution should accomplish two general goals (the "Goals"): first, the statute should address the risks created by the vulnerabilities, force the internalization of the cost of risk, and thus initiate the Cycle of Improvement. Second, the statute should *efficiently* handle the process of allocating losses and making parties whole, two tasks at which arbitration has failed. Figure 1 lists the five identified vulnerabilities and summarizes (1) who has the power to minimize or eliminate the risk, (2) the degree of difficulty in fixing damages for loss, and (3) the critical issues which should be addressed by any proposed legislation.

¶49 The chart in Figure 1 suggests two general strategies (the “Strategies”). First, the power to eliminate or minimize the risk associated with Cybertrading lies almost exclusively in the hands of the Cyberbrokerages. Still, traders must meet minimum reasonableness standards, such as safeguarding passwords, and exhibiting a basic understanding of how the Internet, their browsing and email software, and their Cyberbroker’s trading system operate. Therefore, the protective legislation should be aimed primarily at pushing brokerages into the Cycle of Improvement, and secondarily, at encouraging traders to behave at or above a minimum acceptable level. Second, the remedy must reflect the fact that damages are easy to fix in some actions, and more difficult to fix in others. Therefore, where determining damages is easy, a “make whole” approach should apply, putting traders in the position they would have been in had the error not been made. For all other claims, a statutory damages approach should be utilized.

Figure 1

	Ability to eliminate or control the risk in the hands of:	**Fixing damages is easy or difficult:**	**Critical issues:**
Difficulty of access or complete interruption of service	Broker	Difficult	System must be up and available; system must be able to handle peak capacity; Cyberbrokerage must not falsely advertise response time.
Losses caused by hackers	Broker Trader[1]	Easy Difficult[2]	Protection against unauthorized withdrawals; protection against bogus trading by hackers; reduction of hacking incidents through control of hiring.
Errors attributable to software	Broker	Easy	Protection against trades executed in error or other losses caused by software failure.
Reliance on erroneous information	Broker Trader[3]	Easy Difficult[4]	Dealing with the two types of reliance issues: first, where the user *does* act, and second, where she *does not* act.
Failure to mitigate damages	Broker	Easy	Establishing procedural mechanism under which Cybertraders can easily access brokerage to report problems; setting forth Cyberbrokerage response time.

[1] While generally brokers may fortify their systems to guard against losses due to hacking, traders share some responsibility. They must take reasonable precautions to keep their access passwords secret, to exit their browsers after working on a public system, and so forth. A statutory solution must account for this shared responsibility.

[2] Fixing damages is difficult in the case of denial-of-service attacks, where traders cannot access the system.

[3] The trader must be held to some reasonableness standard. While it is generally true that a Cyberbroker controls the accuracy of the price information it posts, at some point the trader must be held to an objective standard. For example, it is not reasonable for a trader to believe she will receive $10,000 per share for a security recently trading at $10. Such a standard might be imposed by capping recovery at a fixed percentage above the trading price.

[4] As stated, reliance losses are easy to fix when they result in positive action. An example is where a trader makes a trade due to a misstated price. It is where the trader *refrains* from making that trade that fixing damages is difficult.

¶50 To fully accommodate the Goals and Strategies, the new legislation should have eight general provisions: (1) a licensing requirement, enabling the SEC to watch over Cyberbrokerages, to ensure that they maintain minimum operational standards and adhere to advertised promises; (2) a system availability requirement, setting forth standards for system capacity and service interruptions (when they operate below these standards, Cyberbrokerages should face financial penalties, and, ultimately, revocation of licenses); (3) protection against unauthorized withdrawals and trade activity; (4) protection for easily quantified errors, i.e. for multiple trades, or for trades executed in reliance on the wrong price; (5) protection, in the form of statutory damages, for losses resulting in damages that are hard to set; (6) reporting procedures and response deadlines; (7) a provision establishing criminal liability, and imposing civil disgorgement and penalties for fraudulent claims; and (8) standards for pre-employment background checks and a provision allowing brokers to insure against technology risks. Figure 2 sets forth a model statute.

¶51 The figures in this model legislation are not based on particular metrics. Further research would be necessary to refine values for system capacity, dollar amounts of fines, and so forth. Such research is beyond the scope of this Note.

Figure 2

§ 1.01 Licensing of Cyberbrokerages

> Prior to offering Cyberbrokerage services, a securities brokerage shall (i) be a registered member of the Securities and Exchange Commission ("SEC") and (ii) file a statement of intent with the SEC. The SEC, in turn, shall issue a license (the "Operating License") to the brokerage, provided that the applicant meets the minimum operating conditions set forth in this statute. If at any time the Cyberbrokerage, either intentionally or negligently fails to meet the standards set forth in this statute, the Operating License shall be cancelled. The SEC, shall give the Cyberbrokerage written notice of its intent to cancel the Operating License, and no less than fourteen calendar days in which to cure the defect which caused the notice to be issued. During this fourteen-day period, the Cyberbrokerage shall not open any new accounts. If an Operating License is cancelled, the Cyberbrokerage shall be eligible to reapply for a new Operating License, provided that the Cyberbrokerage can demonstrate that it meets all minimum operating conditions set forth herein.

Licensing is an integral part of a plan to establish minimum operating standards. The licensing standard serves two functions. First, it ensures that at the time of licensing, the Cyberbrokerage meets the minimum standards set forth in the statute. Second, it provides an incentive for the Cyberbrokerage to adhere to these standards on a continuing basis. If the broker fails to do so, it faces two escalating penalties. First, it is prevented from accepting new customers; later, its license is subject to cancellation.

§ 1.02 System Availability

> (a) System Capacity – Minimum Requirement. The Cyberbrokerage's operating system shall be capable of handling simultaneous use by at least 50% of the total number of registered account holders. The Cyberbrokerage, at its expense, shall have an independent auditor verify compliance with this condition each calendar quarter. Within 10 days of the end of each calendar quarter, the Cyberbrokerage shall deliver to the SEC a copy of this audit, which the SEC shall make available to the public. Failure to submit this certificate, or submission of a certificate indicating that the Cyberbrokerage does not meet the conditions set forth in this subsection, shall constitute a failure to meet the minimum operating standards set forth in this statute.
>
> (b) Restrictions on Advertising. If the Cyberbrokerage publishes commercial advertisements which make claims concerning the speed of access, the speed of execution of trades, or the hours of system availability, then the Cyberbrokerage shall be responsible for submitting a copy of this advertisement to the SEC, along with an independent auditor's statement verifying that the available service substantiates each claim. For purposes of this subsection, the Cyberbrokerage's claim shall be satisfactory and valid if the advertised level of service is available in at least 98 of 100 service request attempts, as conducted by the independent auditor, provided that those service request attempts are made from at least 10 different geographical points within the area in which the Cyberbrokerage has advertised. The publication of any

> advertisement not meeting the qualifications set forth in this subsection shall constitute a breach of the minimum operating standards set forth in this statute, whether or not the claim meets the service standard set forth herein.
>
> (c) Service Interruptions. The Cyberbrokerage shall report to the SEC, within 10 days following the conclusion of any period of service interruption, the details of the service interruption, including the date and time the interruption started, the date and time the interruption ended, and the nature of the interruption. No Cyberbrokerage will be in violation of this subsection for system interruptions which occur outside the usual hours for market trading, provided that the Cyberbrokerage indicates clearly to its members that its system will not be available at certain regular times of day, and the interruption coincides with the appointed, published time. Excepting the preceding provision, if a Cyberbrokerage's system fails to meet the following standards of availability, the Cyberbrokerage will be deemed to have breached the minimum operating standards set forth in this statute if:
>
> 1. The system is unavailable for more than an aggregate total of 10 minutes, during market open hours, during any continuous thirty-day period; or,
> 2. The system is unavailable for more than an aggregate total of 8 hours during any continuous thirty day period; or,
> 3. The system experiences 10 or more service interruption incidents, or 2 or more such incidents during market open hours, during any continuous thirty-day period.

The system availability provision is designed to mitigate three of the critical issues that have been identified. First, by ensuring that Cyberbrokerages' operating systems are able to handle fifty percent of their user base simultaneously, traders will be assured of satisfactory access to their accounts even during periods of peak market activity. This is a dramatic improvement upon currently deployed operating systems.[117] Second, advertising restrictions will ensure that access and trade claims are accurate. This eliminates reliance on deceptive information, and has the secondary effect of slowing user base growth when systems are at capacity (at such times, the Cyberbrokerage will be unable to advertise speedy access and trade times, which should cool registration of new of users). Third, the service interruption provision sets bright-line availability standards, focusing on near-perfect availability during market open hours, when access is most critical. Cyberbrokerages will be required to maintain 24-hour access, unless they clearly notify users that their system will be regularly unavailable after close of trading on the relevant exchanges.

§ 1.03 Protection Against Unauthorized Withdrawals and Trade Activity

> (a) Unauthorized Withdrawals. Unauthorized withdrawals from any Cyberbrokerage account made by any technological means, whether by debit card or otherwise, excepting any fraudulent withdrawals made in person or by mail, shall be afforded the remedies outlined in the Electronic Funds Transfer Act, 15 U.S.C. § 1693 (2000). A Cybertrader shall be liable for no more than $500 of any such unauthorized withdrawal.
>
> (b) Unauthorized Trading Activity. A Cybertrader shall not be liable for trades placed on her account without her permission, beyond the first $500 of any such loss. This $500 liability shall not be imposed more than once during any twelve-month period. The Cybertrader shall at all times keep her Personal Identification Number (PIN) secure. Upon notification of unauthorized trading activity, the Cyberbrokerage shall reverse such unauthorized activity within thirty calendar days, restoring the account to the position it would have been in had the unauthorized activity not occurred. The Cyberbrokerage may decline to take action under this section, and in this case must offer the Cybertrader the option to proceed to arbitration, if the Cyberbrokerage believes that either (i) the claim is fraudulent or (ii) the Cybertrader acted negligently with respect to securing her PIN. If the Cyberbrokerage so elects, it must issue a credit nonetheless to restore the account to its original position, pending the outcome of the arbitration. Arbitration expenses are to be paid by the Cyberbrokerage. Cybertraders knowingly filing erroneous claims under this subsection shall be liable for fraud under section 1.07 of this statute.

Although losses due to unauthorized withdrawals and bogus activity by hackers have not been a major problem yet,[118] a statutory solution should provide protection against these activities. EFTA has been successful in protecting consumers against unauthorized withdrawals occurring by way of ATM fraud or electronic transfer fraud.[119] Because unauthorized withdrawals from brokerage accounts are similar in nature (in fact, fraudulent online charges are often accomplished by way of debit cards[120]), the remedies set forth in EFTA should be applied to unauthorized withdrawals from brokerage accounts.

Statutory protection should also shield Cybertraders from liability arising from unauthorized trading by hackers. This provision may be abused: Cybertraders who place losing trades may report the trades as fraudulent to avoid the loss. However, holders of ATM cards can also withdraw funds from their accounts and seek remuneration under the auspices of EFTA. The mere possibility of consumer fraud by a minority of consumers should not deter an effort to protect the majority. Protection of this type is warranted by the expected proliferation of computer crime. The provisions set forth in section 1.07 of the statute provide for a severe remedy for fraud; this provision will adequately deter trader misconduct.

§ 1.04 Trades Executed Due to Cyberbrokerage's Error; Trades Executed in Reliance on Erroneous Information

> (a) Cyberbrokerage's Liability for Erroneous Trades. If a Cyberbrokerage, by its own error, processes a trade mistakenly, including processing of cancelled trades, multiple processing of the same trade order, processing a trade on an incorrect account, or processing a trade at an incorrect price, the Cyberbroker shall correct the error and place the Cybertrader in the position she would have been in had the trade been executed properly, or not at all, as the case may be. If the.Cyberbrokerage discovers the error, it shall correct the error without a request from the Cybertrader. If the Cybertrader discovers the error and reports it within ten calendar days of the error's occurrence, and prior to corrective activity taken under this subsection by the Cyberbrokerage, the Cybertrader shall be entitled to additional damages of $250. If a Cybertrader has notice of an error but fails to report it within thirty calendar days after such notification is received, she will be entitled to the remedy set forth in this subsection, less $250, or to no remedy if the value of the error is less than $250.
>
> (b) Cyberbrokerage's Liability for Posting Erroneous Information Resulting in Trade Activity. A Cybertrader shall be entitled to the remedy set forth in section 1.04(a) when a Cyberbrokerage posts incorrect trade information and the Cybertrader places a trade based on this information, as long as the trade occurs in reliance on the information, and, in any event, not later than four hours after receiving the erroneous information, and, provided furthermore, that the Cybertrader shall not be entitled to any additional damages as specified in section 1.04(a). A Cybertrader is not eligible for protection under this subsection if the erroneous price is one hundred times greater than or less than the actual price of the security at the time of the error.

The purpose of section 1.04 is to provide a remedy for losses that result in easily quantified damages, and simultaneously encourage Cybertraders to meet minimum standards of behavior to secure compensation. The section applies a "make whole" approach; traders should be put in the position they would have been in had the erroneous activity not taken place. In addition, the section imposes incentives and disincentives for certain types of behavior in reporting errors or relying on information. For example, Cyberbrokerages are encouraged to uncover and correct errors themselves; if a Cybertrader discovers an error before the brokerage, she is awarded $250 for her effort. On the other hand, if the Cybertrader does not report the error within a reasonable period of time, she is subjected to a $250 penalty. For reliance actions resulting in trade activity, it is deemed unreasonable to act on market information more than four hours old, or to rely on grossly erroneous information. The trader is penalized if she does so.

§ 1.05 Posting Erroneous Security Price Information Not Resulting in Trade Activity; Posting of Incorrect Account Balance

> If a Cybertrader is presented with incorrect price information for a security, or incorrect balance information for her account, she may submit a browser printout showing the web address, date, time, and the display of the screen bearing the incorrect information, along with documentation of the actual price of the security or actual account balance at that time, or, if no such documentation is available, a written explanation describing why she believes the browser printout is incorrect. This information shall be submitted to the Cyberbrokerage in writing within forty-five days of the posting of incorrect information. Upon receipt of this information, the Cyberbrokerage shall either (i) pay $250 to the Cybertrader, or (ii)

> explain in writing why the claim is rejected. The only valid reasons for rejection of a claim are (i) that the posted price or account balance was the correct price at the time it was posted, or (ii) the Cybertrader has been paid $250 pursuant to this subsection within the last twelve months. The Cybertrader may file a claim in any small claims court in which jurisdiction is proper to enforce her rights under this subsection.

Losses are difficult to quantify where erroneous information is posted but no trade activity follows. Yet the statute should nevertheless encourage Cyberbrokerages to post accurate information at all times. Therefore, section 1.05 sets up a system of statutory damages, creating an incentive for brokers to post correct information. The methods of proof are simple. For example, to prove an "erroneous information" claim, the claimant need only print the browser screen[121] and mail it in with proof of the correct price or account balance. Disputes are funneled to small claims court, a common strategy where statutory damage statutes provide for low-dollar damages.[122] A provision limiting the number of collections possible under section 1.05 prevents a trader from mining the system for errors, to make a living out of bounty collections.

§ 1.06 Reporting Procedures and Response Guidelines

> (a) Reporting Procedures. To meet the minimum operating requirements herein, a Cyberbrokerage shall operate a toll-free telephone response center, available twenty-four hours a day, daily, for purposes of fielding reports of problems. If a service interruption affects the Internet operating system during regular hours for market trading, the Cyberbrokerage shall deposit into the account of each account holder $1 for each sixty-minute period of interruption or portion thereof. The Cyberbrokerage shall not be required to deposit this amount if it has the ability to direct traders to its toll-free call center during such an outage. If the call center can provide live, in-person service within five minutes of connection in eighty percent of cases, the Cyberbrokerage shall not be liable for the monetary damages set forth in this subsection. Nothing in this section shall be interpreted as preventing Cyberbrokerages from sharing call centers or employing outside vendors to provide call center services. Callers reporting problems shall receive a unique reporting identification number, and the Cyberbrokerage shall keep a log of the numbers assigned, along with the date and time of assignment, and records of all correspondence and other communication relating to problems. This log shall be available for inspection by the general public at the principal place of business of the Cyberbrokerage during normal business hours.
>
> (b) Response Times. A Cyberbrokerage shall respond to any inquiry by an account holder who notifies the Cyberbrokerage of a problem, error, or claim as to the trader's account, within five business days of receipt of the inquiry, or sooner if possible. If the Cyberbrokerage fails to respond in that time, then (i) a rebuttable presumption shall arise that the inquiry shall be resolved in favor of the claimant, and (ii) the Cyberbrokerage shall pay the claimant $250.

There are two purposes to section 1.06. First, Cyberbrokerages are encouraged to maintain call centers where traders can place trades when the online systems are unavailable. If they do so, the brokerages are released from statutory damages for system interruption incidents. The call centers also serve as a point-of-contact for error resolution, helping consumers to quickly deliver error information to the broker, which mitigates damages. Brokerages may share call centers or hire outside call center providers to reduce the cost of delivering this service. Second, response time provisions ensure that consumer complaints are handled quickly; again, the goal is to mitigate damages and provide for prompt resolution of errors. Statutory damages create an incentive for the broker to make a timely reply.

§ 1.07 Cybertrader's Liability for Fraud

> A Cybertrader fraudulently filing a claim under this section shall be guilty of a felony. Additionally, upon a showing of fraud in a civil action, by a preponderance of the evidence, a court of law is authorized to order disgorgement of any illegitimately obtained funds, along with a fine not to exceed $100,000, plus court costs and attorneys' fees.

Section 1.07 is designed to provide strict criminal and civil penalties for fraud. As this statute is designed to spread the cost of risk across the entire base of traders, amplification of per-user costs due to increased fraud cannot be tolerated. Where individuals are responsible for harming the trading community by contributing to losses, they should be penalized. Section 1.07 provides a sufficient disincentive to engage in such behavior.

§ 1.08 General Provisions

> (a) Insurance. Nothing in this subsection shall be construed to mean that Cyberbrokerages may not utilize insurance products to insure against any liability or potential liability arising under this statute. However, the procurement of insurance shall not waive any duty of the Cyberbrokerage herein.
>
> (b) Employment Standards. Cyberbrokerages shall conduct a reasonable background inquiry, and make a reasonable hiring decision based upon the finding of such background inquiry, for every employee who has access to the use of any of the Cyberbrokerage's computer systems, or to any account information.

Cyberbrokerages should be allowed to insure against losses arising from any of the vulnerabilities delineated herein, so long as the procurement of insurance does not waive any compliance requirements. The procurement of insurance reflects a decision by the brokerage that paying a fixed cost for risk is more efficient than paying a variable cost. The cost is internalized whether fixed or variable. Therefore, insurance does not detract from consumer benefit and should be allowed.

Brokerages should be required to conduct reasonable background checks on prospective employees, and to act on the results of these inquiries. Prior to implementing this statute, Congress should delineate what constitutes a reasonable inquiry. Given that often hacker attacks are initiated by employees, the implementation of background checks will serve to lessen the frequency of attacks.

V. Conclusion

¶52 Congress has historically introduced consumer protection legislation designed to mitigate risks to consumers inherent in the use of new financial services technologies. This kind of legislation has been successful, in that it has encouraged service providers to enhance security systems and take other steps to minimize losses arising from the use of the technology, while simultaneously protecting consumers from large, individual losses. When properly designed, the costs imposed by such legislation are high enough to encourage service providers to make needed security improvements, but not so high as to make the provision of the service unfeasible. While one might perceive the added cost as a threat to the very existence of the service, in the cases of ATM and credit cards, user bases have expanded subsequent to passage of protective legislation, leading to greater profits for card issuers even after accounting for the costs imposed by the legislation.[123] Cybertrading is a widely used new technology, which gives rise to unique vulnerabilities. Given the success of past legislation, and the lack of a suitable existing statute, Congress should adopt consumer protection legislation to protect Cybertraders. The costs imposed on Cyberbrokers should be carefully planned to create the desired result.

[†] Boalt Hall, J.D. candidate 2002.

[1] Henrique de Azevedo Ferreira Franca, *Legal Aspects of Internet Securities Transactions*, 5 B.U. J. SCI. & TECH. 4, 5 (1999).

[2] *See* Martin J. Aronstein et al., *Article 8 Is Ready*, 93 HARV. L. REV. 889, 890 (1980) (acknowledging the paperwork problems of the securities industry).

[3] *See* Charles W. Mooney, *Beyond Negotiability: A New Model for Transfer and Pledge of Interests in Securities Controlled by Intermediaries*, 12 CARDOZO L. REV. 305, 317 (1990) (discussing the establishment of the Depository Trust Company, one of the largest clearing corporations).

[4] *See* Aronstein et al., *supra* note 2, at 891.

[5] David A. Kessler, *Investor Casualties in the War for Market Efficiency*, 9 Am. U. Admin. L.J. 1307, 1329 (1996).

[6] Securities Investor Protection Act (SIPA), Pub. L. No. 91-598, 84 Stat. 1636 (codified as amended at 15 U.S.C. § 78 (1994)).

[7] *See generally* Electronic Fund Transfer Act (EFTA), Pub. L. No. 95-630, 92 Stat. 3728 (codified as amended at 15 U.S.C. § 1693 (2000)) (protecting consumers from liability from fraudulent electronic fund transfer transactions); *see also* Truth In Lending Act (TILA), Pub. L. No. 90-321, 82 Stat. 146 (codified as amended in scattered sections of 15 U.S.C.) (establishing liability limits for fraudulent use of credit cards).

[8] *Id.*

[9] Taken from a list of top brokers ranked Gomez.com, a preeminent web rating service, *at* http://www.gomez.com/scorecards/index.asp?topcat_id=3&subSect;=finance. (last visited Mar. 6, 2001).

[10] Lexis-Nexis search on Nov. 5, 2000.

[11] Based on quarterly filings of the top ten Cyberbrokers, *see* Gomez.com, *supra* note 9, utilizing the most recent 10-Q or 10-Q/A filing, http://www.nasdaq.com. (last visited Mar. 6, 2001).

[12] *See* Pl.'s Compl., Cooper v. E Trade Group, Inc.., No. CV770328 (Cal. Super. Ct. filed Nov. 21, 1997), http://securities.stanford.edu/complaints/etrade/cv770328/001.html (last visited Mar. 6, 2001).

[13] *See* Greg Ip, *Firms Often Leave Investors at Mercy of Computer Error*, Wall St. J., June 6, 2000, at B1.

[14] *Id.*

[15] *Id.*

[16] *Id.*

[17] Based on the most recent quarterly filings, as of Nov. 5, 2000, for Charles Schwab, E*Trade, Fidelity Investments, DLJ Direct, TD Waterhouse, National Discount Brokers, American Express Brokerage, Merrill Lynch Direct, My Discount Broker and Suretrade, http://edgar-online.com (last visited Mar. 6, 2001).

[18] *See* Gomez.com, *supra* note 9.

[19] *See* Nasdaq.com, *supra* note 11.

[20] Lexis-Nexis search on Nov. 6, 2000, evidencing, for example, 5 individual arbitrations for E*Trade alone.

[21] Ianthe Jeanne Dugan, *Glitch Idles E-Trade Customers*, Wash. Post, Feb. 4, 1999, at E1 ("The [E*Trade] setback occurred just a week after SEC Chairman Arthur Levitt Jr. disclosed 330 complaints about online transactions that could not be processed, blaming much of the problem on firms accepting more business than they could handle.").

[22] *See, e.g.*, Aidikoff & Uhl, *at* http://securitiesarbitration.com (last visited Mar. 6, 2001).

[23] *See* Dugan, *supra* note 21 (stating that E*Trade attributed a recent problem to a malfunction of new 'trading functionality' software).

[24] *See Glitches Dog E*Trade for Second Day*, CNBC.Com, Feb. 4, 1999 (stating that the surge in Internet trading has led to many outages at brokers), http://www.securitiesarbitration.com/success/success_16.htm (last visited Mar. 6, 2001); *see also* Dugan, *supra* note 21 (noting that the Chairman of the SEC blames crashes on brokerages accepting more business than they are technically capable of handling).

[25] *See* Troy Wolverton, *E*Trade Fixes One Security Problem, Admits Another*, CNET News.Com, Sept. 26, 2000 (stating that E*Trade learned about a major security problem, and was quickly acting to fix the problem), *at*

http://news.cnet.com/news/0-1007-202-2870712.html; *see also* Danielle Fugazy, *Security: Protect Web Sites and Data, Executive Says*, Web Finance, Apr. 24, 2000 ("No one was prepared for the denial of service attacks that took place a months ago because it was not on executives' radar screens…").

[26] *See* Mitch Wagner, *Casting a Wide Net for Web Talent-Companies Reassign Workers, Tap Internal Referrals and Internet Job Sites to Ease Shortage*, InternetWeek, Oct. 30, 2000.

[27] *See* Wolverton, *supra* note 25.

[28] *See* Nicole O. Coulter, *Inexperience at Online Firms May Jeopardize Investors*, Horsemouth.Com, Aug. 10, 2000 (stating that E*Trade's failure to take corrective action for forty days caused additional losses), http://www.securitiesarbitration/success/success_40.htm (last visited Mar. 6, 2001).

[29] *See* Nasdaq.com, *supra* note 11.

[30] *Id.*

[31] *Id.*

[32] Susan Pulliam & Dave Pettit, *Legal Claims By Online Traders Are On the Rise as Market Turns Stormy*, Wall st. J., July 16, 2000, at B2.

[33] *See* Pl.'s Compl., *Cooper*, *supra* note 12.

[34] Based on an examination of pending class action complaints disclosed in SEC reports, *see* Nasdaq.com, *supra* note 11. A list of class actions is available at http://securities.stanford.edu (last visited Mar. 6, 2001).

[35] *See* Pl.'s Compl., *Cooper*, *supra* note 12 ("E*Trade's growth has outstripped its ability to provide convenient and rapid securities trading to its customers.").

[36] *Id.* ("Despite this knowledge, during the quarter ended September 30, 1997, E*Trade launched a $25 million multi-media marketing advertising campaign.").

[37] *See* Ip, *supra* note 13 ("E*Trade kept spending heavily on marketing early last year even as the crush of activity strained its and other brokers' capacity, while competitors Ameritrade and T.D. Waterhouse Group Inc. said they pulled back.").

[38] *See* Pl.'s Compl., *Cooper*, *supra* note 12.

[39] *Id.*

[40] *Id.*

[41] *See id.*; *see also* Victoria Colliver, *Consumers' Sense of Security Dented by Internet Vandals, But Most Won't Change Online Habits*, S.F. Exam'r, Feb. 10, 2000, at B1.

[42] *FBI Begins Probe of Web Assaults*, Indianapolis Star, Feb. 10, 2000, at A1; *see also* Colliver, *supra* note 41.

[43] *See* Pl.'s Compl., *Cooper*, *supra* note 12 (discussing the heavy market activity on Oct. 27 and 28, 1997).

[44] *Id.*

[45] *Id.*

[46] *Id.*

[47] *Id.*

[48] Ip, *supra* note 13 (stating that E*Trade was involved in fifty-one arbitrations in a recent monitoring period; only Schwab had more, at eighty, but Schwab also had nine times as many accounts).

[49] Lisa Salters & Don Dahler, *Morning Business Report*, ABC WORLD NEWS THIS MORNING (No. 99083104-j03), Aug. 31, 1999.

[50] Stephen Miles, *Land of the $5 Trade: When It Comes to Dealing with US Discounters, the Grass Isn't Necessarily Greener - But It's Definitely Cheaper,* NATL. POST, Feb. 26, 2000, at C4.

[51] Dugan, *supra* note 21.

[52] Per examination of SEC statements available on Nov. 5, 2000, *supra* note 11.

[53] Molly McMillin, *Fidelity Bank in Wichita Suspends Use of Debit Cards*, WICHITA EAGLE, Nov. 19, 1998, at 6.

[54] Michael Braga, *Online Brokerages Offered Help Fighting Computer Hackers*, BROWARD DAILY BUS. REV., Dec. 7, 1999, at A1.

[55] Kevin Grace, *No Such Thing as Privacy: The Internet is Your Window on the World, and the World's Window on You*, CAN. BUS. & CURRENT AFF., Feb. 28, 2000, at 3.

[56] Examination of SEC reports, news media, and arbitration filings on Nov. 5, 2000, *supra* note 11.

[57] *See generally* Christopher Null, *How to Hire a Hacker*, ZIFF DAVIS SMART BUS. NEWS FOR THE NEW ECON., July 1, 2000, at 112 (quoting expert John Klein of "Hire a Hacker," a consulting and protective service); *see also* Fugazy, *supra* note 25 (quoting Jerry Archer, vice president of information security for Fidelity Investments); *see also* McMillin, *supra* note 53 (quoting William Jones of Intrust Bank).

[58] Fugazy, *supra* note 25.

[59] *Id*.

[60] *Id*.

[61] *National Discount Brokers Group Discusses Recent Disruption of Services at NDB.com*, PR NEWSWIRE, Mar. 2, 2000 [hereinafter *National Discount Brokers*].

[62] Rodd Zolkos, *Most Cyberterrorists are Unhappy Employees*, INVESTMENT NEWS, Mar. 6, 2000, at 13.

[63] *Id*.

[64] Mark Slater, *Viruses, Hackers and Outages: Who Pays?*, MAELEY'S CYBER TECH LITIG. REP., June 2000, at 6; *see also* James Brewer, *Insurance Review: Fraud-Keeping It Safe in an Online Environment*, LLOYD'S LIST, Apr. 28, 2000, at 8.

[65] Salters & Dahler, *supra* note 49 (stating that Schwab admitted that a half-hour system outage, which left millions of people without access to their accounts during market hours, was caused by a software glitch).

[66] *National Discount Brokers*, *supra* note 61 (noting that National Discount Brokers was forced to work with software vendor to solve problem that made Cybertrading system vulnerable to hacker attacks).

[67] *See generally* the SEC reports and arbitration claims, *supra* note 11.

[68] Ip, *supra* note 13.

[69] *Id*.

[70] *See id*.; *see also* Pl.'s Compl., *Cooper*, *supra* note 12 (stating that the failure to send confirmations within twenty-four hours led to additional trades).

[71] *E*Trade Securities, Inc. Found Liable and Ordered to Compensate On-Line Investor Morgan Roach*, PR NEWSWIRE, Oct. 30, 2000 ("Mr. Roach proved that E*&Trade misstated the pricing of America Online options during AOL's merger

with Netscape.").

[72] Ward Lassoe & Garrett Glaser, *Web Site Raises Question of Conflict*, CNBC.COM, Apr. 9, 1999 ("One stock was… selling for about $2 a share. Wilson says he jumped in to buy 2,000 shares. But because trades on the Internet are not instantaneous, as he waited for the confirmation of the market order from his on-line broker, he says, the stock price took off…[he] got an execution at [$]10.").

[73] *See* Ip, supra note 13 (discussing trader Scott Shields, whose $12,200 account showed a balance of $2.4 million when, in reality, he was *losing* the $12,200 principal).

[74] Pl.'s Compl., *Cooper*, *supra* note 12.

[75] *See, e.g.*, Ip, *supra* note 13 (explaining how trader William Badgerow's 5,000 share trade was executed twice in error, and then Badgerow was kept on hold for at least three and maybe as many as seven hours as market price continued to fall, exacerbating the loss).

[76] Coulter, *supra* note 28.

[77] *Id*.

[78] *Id*.

[79] *See generally* 15 U.S.C. § 1601 (2000) (TILA); 15 U.S.C. § 1693 (2000) (EFTA); 15 U.S.C. 78 (2000) (SIPA).

[80] SIPC, *SIPC AND CUSTOMER PROTECTION* (Jan. 1995), http://www.sipc.org/publications/index.html (last visited Mar. 6, 2001).

[81] Philip Aidikoff, *SIPC's Role in Protection from Fraud Examined*, DESERT SUN, Sept. 24, 2000, at B1 ("The SIPC provides limited protection for unauthorized transactions.").

[82] SIPC, *supra* note 80.

[83] Kessler, *supra* note 5, at 1318.

[84] SIPC, *supra* note 80.

[85] *Id*.

[86] *Id*.

[87] *Id*.

[88] 15 U.S.C. § 1601 (2000).

[89] 15 U.S.C. § 1643(a)(1)(B) (2000).

[90] Jeffrey Kutler, *Fed Staff Considers Raising $50 Limit on Card Liability*, AM. BANKER, Oct. 31, 1980, at 1.

[91] *Consumer Groups Say ATM Operations Need More Regulation to Halt Crime; Forces in Marketplace Will Solve Problems, Operators Argue*, AM. BANKER, July 17, 1984, at 32 [hereinafter *Consumer Groups*] (quoting Mark Leymaster of the National Consumer Law Center, "'…[B]anks have to make cold-blooded business decisions, and they will continue to do so on the other side of the consumer… [U]nless we have minimum consumer protections, we will have continuous abuses of the customer.'").

[92] *Electronic Banking*, BUS. WK., Jan. 18, 1982, at 70 ("Suddenly, the picture changed. ATMs became cheaper and more reliable, and bankers were astonished to discover that the lines behind their machines were becoming as long as those at the teller windows. The growing consumer acceptance brought an explosive demand for the machines, and the installed ATM base has nearly doubled in the past two years.").

[93] *See Consumer Groups*, *supra* note 91 (quoting Mark Leymaster of the National Consumer Law Center, "'Banks have all the control in ATM transactions. The line is frequently drawn against the consumer when practical problems arise with these machines. In the ambiguous situations, the consumer loses unless someone intervenes.'").

[94] *Id.* ("After about 125 Citibank customers failed to get refunds from the bank, New York State Attorney General Robert Abrams brought a class action suit against the institution.").

[95] *See, e.g.*, Robert D. Hershey, Jr., *Drop in Computer Issues Hammers Nasdaq for 83.34 Fall*, N.Y. TIMES, Feb. 5, 1999, at C7.

[96] 15 U.S.C. § 1693 (2000).

[97] *See* Catherine England, *The Case for Banking Deregulation*, HERITAGE FOUND. REP., Mar. 26, 1982.

[98] 15 U.S.C. § 1693(g) (2000).

[99] 15 U.S.C. § 1693(f) (2000).

[100] *See* Clayton P. Gillette, *Rules, Standards and Precautions in Payment Systems*, 82 VA. L. REV. 181, 208 (1996).

[101] *See, e.g.*, Visa, *Zero Liability*, *at* http://www.visa.com/av/zero_liability/main.html (last visited Mar. 6, 2001).

[102] Jason Anders, *Disputes With Online Brokers Could be Frustrating to Resolve*, WALL ST. J. INTERACTIVE ED., June 28, 1999 ("Most brokerage agreements require disputes between a firm and its clients to be settled through industry-sponsored arbitration - fine print that many investors probably never pause to read when they open an account.").

[103] *Id.* ("Arbitration became widely embraced after a 1987 Supreme Court ruling affirmed its use for settling securities matters.").

[104] *See, e.g.*, Kingston v. Ameritrade, 12 P.3d 929 (Mont. 2000) (remanding for finding of fact as to whether plaintiff received notice that the arbitration clause bound him).

[105] Anders, *supra* note 102.

[106] *Id.*

[107] Stuart Silverstein, *NASD's Bumpy Road to Justice*, L.A. TIMES, July 27, 1999, at C1.

[108] *Id.*

[109] *Id.*

[110] *Id.*

[111] *Id.*; *see also* Pulliam & Pettit, *supra* note 32 ("In every case that a customer brings, the brokerage firm will be represented by a lawyer. 'No matter how good you are, if you are up against a skilled attorney, you really are at a disadvantage.'").

[112] *Id.*

[113] *See Consumer Groups*, *supra* note 91.

[114] *See* Gillette, *supra* note 100 (stating that ATM card issuers earnings increased even after accounting for regulatory costs imposed by protective legislation, due to an increase in the user base).

[115] *See, e.g.*, Laurel Pallock, *New Credit Card Scams*, S.F. CHRON., Jan. 9, 1991, at A1 (describing counterfeiters' reactions to hologram logos on credit cards).

[116] *See* Gillette, *supra* note 100.

[117] *See Pl.'s Compl., Cooper*, *supra* note 12 (stating that E*Trade's system reportedly can handle only 7% of its users simultaneously).

[118] Per examination of SEC statements, *supra* note 11.

[119] *See generally* Margaret Samuel, *Non-Cash Alternatives and Money Laundering: An American Model for Canadian Consumers' Protection*, 30 AM. BUS. L.J. 169 (1992) (advocating adoption of EFTA-style legislation in Canada).

[120] *See* McMillin, *supra* note 53.

[121] Printouts of browser screens, along with telephone bills showing online activity, have been successfully used in the past to demonstrate such errors. *See* Pulliam & Pettit, *supra* note 32.

[122] *See, e.g.,* Cal. Civ. Code § 1722(a)(2) (2001) (providing statutory damages of up to $500 for utility company's failure to adhere to four-hour appointment window).

[123] *See* Gillette, *supra* note 100.