2001

Symposium, Mutual Funds and the Protection of Shareholder Accounts

Larry D Barnett

MUTUAL FUNDS AND THE PROTECTION OF SHAREHOLDER ACCOUNTS

LARRY D. BARNETT*

How secure are shareholder accounts at mutual funds in the United States? Given the large number of Americans who have invested in mutual funds and the substantial amount of money in investors' accounts,[1] the question attracts surprisingly little attention. Yet it is a question of pressing importance because mutual funds, generally, now allow their shareholders to acquire account information and effect account transactions through "touch-tone" telephone systems, and, increasingly, through personal computers with an Internet connection.[2] This article focuses on the potential that automated telephonic systems and the network of computers known as the Internet create for deliberate, unauthorized intrusions into shareholder accounts. In general, the mutual fund industry does not seem to view this potential as serious. If the industry is making an unwarranted assumption, however, there could be sizeable losses and, even more importantly, a diminution of public trust in an important facet of our economy. To the extent that trust in a social institution declines, the institution is weakened and society is less stable.[3]

I. VULNERABILITY OF SHAREHOLDER ACCOUNTS

To illustrate the scope of the possible threat to the security of shareholder accounts, consider the success of a hacker in Russia who, in 1994, penetrated the computer system of Citibank of New York.[4] Over a period of months he was able to transfer an estimated $10 to

* Professor of Law, Widener University. Mailing address: P.O. Box 7474, Wilmington, DE 19810-3221. E-mail address: larry.d.barnett@law.widener.edu.

1. At the end of 1998, fund shares were owned by an estimated 77.3 million individuals in the United States. The market value of the shares held by individuals was $4.3 trillion. INVESTMENT COMPANY INSTITUTE, MUTUAL FUND FACT BOOK 41 (1999), *available at* http://www.ici.org/facts_figures/factbook-99_toc.html.

2. Unfortunately, industry-wide data does not exist on the number of shareholders who have registered for account access by telephone and/or computer.

3. *See* J. David Lewis & Andrew Weigert, *Trust as a Social Reality*, 63 SOC. FORCES 967, 974 (1985).

4. *See* Amy Harmon, *Here We Keep the Hacker Tradition*, L.A. TIMES, July 29, 1996, at D1. *See also* Jennifer Gould, *Hacker Heist*, VILLAGE VOICE, Dec. 23, 1997, at 39.

$12 million from accounts of Citibank customers located in North and South America and Asia to bank accounts of his accomplices in the United States, Israel, Scandinavia, and Europe. Particularly disturbing is that acquaintances of the hacker described him as possessing a mere "third-rate" ability with computers.[5] Hackers with advanced expertise can presumably invade the computer systems of financial institutions that are protected by measures of greater sophistication.[6] However, even if defensive measures for the computers of financial institutions progress to the point where they are completely impenetrable—a point very unlikely to be reached—personal computers used by individuals will remain vulnerable. Because individuals will use personal computers to access their accounts through the Internet, the vulnerability of those computers is a concern.

How susceptible are personal computers to intrusions? One prearranged test found that an expert in computer security could easily acquire files residing on the hard drive of a target personal computer, and passwords transmitted by that computer. The test, indeed, "made hacking look like child's play."[7] However, a high level of proficiency in hacking seems unnecessary, and hackers of just modest ability are apparently capable of obtaining account passwords and other identifying information from personal computers with no difficulty: "Even relatively inexperienced [computer] crackers don't have much trouble breaking into home systems."[8]

Why are personal computers at high risk of being penetrated by hackers? The vulnerability stems from numerous factors, including two that have recently received attention. First, users of personal computers that have high-speed Internet connections, such as cable modems and digital subscriber lines, may download software that the users do not realize allows remote access to their computers. For example, users may receive e-mail recommending that they download from a designated Web site an update to important software, such as Windows. Installing the program introduces into the computer a "Re-

---

5. *See* Harmon, *supra* note 4.

6. Citibank has maintained that it recovered most of the money stolen by the hacker. However, the theft from Citibank may not be an isolated incident, and other banks may have suffered large (but unpublicized) losses from hacking. *See* Udo Flohr, *Bank Robbers Go Electronic*, BYTE, Nov. 1995, at 48.

7. Paul C. Judge, *What's the Password? Hackers May Already Know*, BUS. WK., Nov. 15, 1999, at 236.

8. Susan Gregory Thomas, *Home Hackers*, U.S. NEWS & WORLD REP., Oct. 4, 1999, at 52, 53.

mote Access Trojan Horse". Given the speed of the Internet connection, this "Trojan Horse" permits others to enter and explore the computer without being detected.[9]

Second, the security of personal computers is impaired by the complexity of computer software and the defects that accompany complexity. Each 1000 lines of software code is estimated to contain an average of five to fifteen flaws.[10] Faulty software increases the vulnerability of personal computers that are connected to the Internet. In 1999, an Internet-transmitted computer virus named Melissa took advantage of an entry point that existed in Microsoft Office software and infected some computers having the software. The virus prompted the computers it infected to send mere bogus e-mail messages, but a virus of greater malevolence could have resulted in serious vandalism by, for example, fabricating financial reports on infected computers and then distributing signed reports from these computers.[11]

Over time, of course, improvements in technology will enhance the security of computers connected to the Internet. Passwords may be abandoned in favor of technology that measures one or more physical attributes to verify that a party who seeks to use or obtain information from a file on a computer is authorized to do so. Such technology may include pads that identify fingerprints and cameras that recognize the iris of eyes.[12] If the expense or character of this technology limits its use to computers in the networks of corporations, software creating a "firewall" may reduce the ability of unauthorized parties to penetrate personal computers. However, firewall software cannot be expected to completely block hackers, who operate over the Internet, since no software can supply complete security. Furthermore, not all personal computers will have the software, and many computers that possess it will be unprotected because the software will have been disabled.

---

9. *See id.* at 53-54.

10. *See* Neil Gross et al., *Software Hell*, BUS. WK., Dec. 6, 1999, at 104, 107.

11. *See id.* at 114. A computer virus named W95.Babylonia, identified in December 1999, has been described as the "first-of-its-kind" because the virus can update itself automatically and hence add new features over time. The virus permits an infected computer to be controlled by the party who created the virus. *See Web Virus Targeting Chat Rooms*, CHI. TRIB., Dec. 8, 1999, at 6.

A virus and a Remote Access Trojan horse can affect computers in similar ways, but the two types of agents differ in a fundamental respect: a virus initiates its own propagation and dissemination, while a Remote Access Trojan horse does not. *See* SYMANTEC CORP., NORTON ANTIVIRUS 2000 USER'S GUIDE 32 (1999).

12. *See* Stephen H. Wildstrom, *Passwords May Soon Be History*, BUS. WK., Nov. 22, 1999, at 22.

At the moment, national governments appear to be years away from a coordinated approach to regulating the Internet and protecting its users. A uniform multination strategy is more likely to restrict Internet mischief, but at least two factors preclude such a strategy for the foreseeable future. One is the concern of law-enforcement agencies that the techniques offering maximum protection for users of personal computers—including individuals accessing their accounts at mutual funds—will seriously hinder the detection of criminal activity and the apprehension of perpetrators. A second factor is the difference between nations in their cultural values, especially with regard to privacy. Security measures that are acceptable in countries where privacy is not highly prized will be rejected in countries where privacy is stressed.[13]

To this point, this article has focused on potential security risks to mutual funds and their shareholders from use of the Internet. While the dimensions of the problem are debatable and solutions will be developed as security problems are detected, new security risks will continually emerge and solutions will not always appear in time to prevent unauthorized intrusions into computers. Accordingly, "worst case" scenarios are important to recognizing possible problems and minimizing the number and magnitude of losses. They need to be considered by the legal profession for two reasons. First, a plausible argument can be made that attorneys for investment companies and their investment advisers are ethically obligated to inquire about the adequacy of security measures and the means that might be implemented to avoid or minimize risks. After all, under the Model Rules, a lawyer may be required to initiate legal advice regarding the practices of a client that are "likely" to have "substantial adverse legal consequence," which apparently include monetary losses for which the client will be liable.[14] This is so even if the advice deals with realities and choices the client would prefer not to face.[15] Second, a lawyer who represents a government-regulated client in a sector of the economy that is important to the financial well-being of the Nation may be liable to that agency for a loss suffered by the client if the lawyer could have reasonably antici-

13. *See* Stephen Baker, *Taming the Wild, Wild Web*, BUS. WK., Oct. 4, 1999, at 154.
14. *See* MODEL RULES OF PROF'L CONDUCT R. 2.1 cmts. 1, 5 (1998).
15. *See id.*

pated the loss and did not act to prevent it.[16] Certain types of economic activity, quite simply, may affect the public interest so directly and so fundamentally that significant failures involving these activities cannot be tolerated. Thus, when the client of a lawyer is a government-regulated organization that supplies a financial service, the needs of the social system as a whole may impose liability on the lawyer for a loss experienced by the client since, with regard to malpractice, a "new world of lawyering" may be emerging in which the interests of society, not the interests of the legal profession, dominate.[17] If so, a lawyer representing a mutual fund or its adviser, even though not directed by the client, ought to be concerned with security practices that could harm the fund and its shareholders.

II. IMPROVING CURRENT SECURITY PRACTICES

There are specific measures that may enhance the security of shareholder accounts. Though some measures may prove impractical for economic or technical reasons, at least on the surface they appear to be reasonable and, hence, warrant consideration. A proposal should not be rejected, of course, merely because it will reduce the profitability of a fund to its investment adviser. In light of the importance of mutual funds to the financial system of the United States and the welfare of Americans, shareholder protection must be the paramount consideration.

What should be the standard for determining the acceptability of a proposed security measure? The answer involves two questions: (1) whether the economic cost of the measure is likely to exceed the economic loss to shareholder accounts if the measure is not implemented and (2) whether a significant diminution of public trust will result from the security breaches that the measure can be expected to avert. The standard is admittedly complex and its application will not be easy. Some degree of judgment is necessary to reach decisions with it. In particular, three variables must be taken into account: the cost to a

16. Traditionally, legal malpractice has required a departure from the degree of skill and care that would reasonably be expected of lawyers in the same jurisdiction. *See* STEPHEN GILLERS, REGULATION OF LAWYERS 699 (5th ed. 1998).

17. *See* Steve France, *Unhappy Pioneers: S&L Lawyers Discover a 'New World' of Liability*, 7 GEO. J. LEGAL ETHICS 725, 728 (1994). One reason that lawyers for governmentally-regulated organizations offering financial services may more often, in the future, be held liable for legal malpractice is that risk management and risk reduction are defining emphases of technologically advanced countries. *See* PETER L. BERNSTEIN, AGAINST THE GODS (1996).

fund of adopting and utilizing a particular security measure, the reduction in losses from security violations that the measure will prevent, and the degree to which security breaches that would have been avoided if the proposal had been implemented will erode public confidence in the fund and the mutual fund industry as a whole. The first and second variables are balanced against one another and require a cost-benefit analysis. The third variable is considered independently.

While an argument may be made that a decision on the acceptability of a security technique should involve only a cost-benefit comparison—and hence be confined to economic considerations—the most important aspect of the proposed standard is its focus on trust, which is a sociological issue. Surprisingly, sociologists have barely studied trust, even with the impressive arsenal of quantitative data and statistical methods they have acquired in the last quarter-century, and the societal function of trust will not be fully understood until a large body of research has been conducted. Nonetheless, trust is undoubtedly "a functional prerequisite for the possibility of society in that the only alternatives to appropriate trust are 'chaos and paralyzing fear'."[18] It is therefore fortunate that the level of trust in institutions, in general, was roughly the same among Americans in the mid-1990s as in the mid-1970s even though the level of trust in particular institutions during this period was diminished by scandal.[19]

While trust appears to be a cornerstone of every society, research is lacking on the factors that reduce or destroy it. However, the susceptibility of trust to erosion probably increases with the density of population, the existence of multiple population centers (i.e., metropolitan areas) that are geographically distant from one another, and the speed with which social and technological change occurs. A densely populated society whose members are separated geographically will be characterized by a relatively low level of face-to-face interaction and, therefore, relationships that often are impersonal. Impersonal relationships, however, are likely to be more fragile and more easily terminated than relationships involving face-to-face contact. Such relationships can therefore be expected to reduce the stability of the social order. Finally, change in technology and social patterns, if rapid and constant, seems apt to destabilize a society by undermining predictability, a prerequisite to sustainable group life.

---

18. Lewis & Weigert, *supra* note 3, at 968.

19. *See* Pamela Paxton, *Is Social Capital Declining in the United States? A Multiple Indicator Assessment*, 105 AM. J. SOC. 88, 117-119 (1999).

In a society where population is dense and dispersed and social and technological change is fast and continuing—as in the United States—trust in institutions may be especially difficult to maintain even though such trust directly affects the efficiency and effectiveness of the social system. Federal securities law allows the recovery of financial losses by shareholders in a mutual fund who have relied on substantially misleading statements or omissions by the fund regarding the securities it issues,[20] but securities law performs a more important function outside the legal system. Law allowing such losses to be recovered preserves trust in institutions and commitment to the social order. When a fiduciary relationship exists—as between the shareholders of a fund and the investment adviser for the fund—statutory or common law must permit the recovery of losses stemming from breaches of fiduciary duties.[21] Otherwise, fiduciary relationships will be less common and, for those relationships that exist, more difficult to maintain.[22] Trust should accordingly be an indispensable factor in decisions regarding the means to minimize risks to shareholders from their investments in mutual funds.

III. CHANGES TO EXISTING SECURITY PRACTICES

Two changes to existing security practices should be considered. Federal securities law and the Uniform Commercial Code may impose liability on an investment company for a loss incurred by a shareholder when the loss stems from an unauthorized account transaction effected by telephone and the company failed to exercise "reasonable care" to prevent the unauthorized transaction.[23] But what security measures are "reasonable"? The suggested changes discussed below may reduce the likelihood that liability will be imposed on mutual funds forced to defend themselves against lawsuits seeking compensation for fraudulent account transactions, that is, the suggested changes may increase the probability that the defendant funds will be deemed to have acted reasonably. Indeed, the suggestions for change, if imple-

20. *See* 15 U.S.C. 77I (1994); *see* also Lucia v. Prospect Street High Income Portfolio, Inc., 36 F.3d 170 (1st Cir. 1994).

21. *See* Lewis & Weigert, *supra* note 3, at 978.

22. *See id.*

23. *See* Investment Company Institute, SEC No-Action Letter (Apr. 19, 1993), *available at* 1993 SEC NO-ACT LEXIS 673. The same standard would presumably apply to losses from transactions by computer over the Internet.

mented, may curb the number of losses from unauthorized account transactions and, hence, avert some lawsuits altogether.

The first suggestion concerns the present ability to direct transactions on fund accounts without speaking to a representative of the fund. Communications by voice can lead a representative to doubt the authenticity of a caller because of peculiar statements, inflections, or other nuances in the caller's speech. If such a doubt arises, the fund representative can pose questions that are designed to determine whether the caller is authorized to conduct transactions on the account to which the caller seeks access. Specifically, the representative can inquire about facts that were elicited on the account registration form, that are available to the representative on the computer of the fund, and that are unlikely to be known by individuals other than those who opened the account. Unfortunately, however, account registration forms rarely gather such facts as date of birth, the name and location of the high school and college(s) from which each account owner graduated, undergraduate and graduate degrees (if any) held by account owners, the fields in which the degrees were earned, and the year of graduation from high school and college (or each college, if more than one). The failure to acquire distinctive information regarding account owners that is not widely available, and to utilize it for the purpose of ascertaining the authenticity of callers, would seem to raise the probability of a finding that reasonable care was not taken to protect the account(s) of a shareholder. Account transactions, therefore, should not be possible except through oral communications with fund personnel.[24]

In addition, fund personnel who deal with shareholders should receive training to recognize situations in which a caller is not authorized to conduct transactions on an account, and the telephone systems used by funds should identify the telephone number from which an incoming call originates in order to ascertain whether it matches a telephone number of any shareholder.[25] When a call is from a telephone number that does not match the account to which access is sought, fund personnel can pose questions of the type described above. To avoid devoting large amounts of time to transactions involving small

24. My suggestion does not necessarily encompass access to account information, since unauthorized acquisitions of information are much less likely than unauthorized account transactions to cause damage.

25. The office and home telephone numbers of each account owner can be (and often are) required on account registration forms.

amounts of money, a fund could require these person-to-person communications only when a shareholder request involves a certain minimum sum (e.g., $2000) or when a series of requests that in the aggregate exceed the minimum are received within a designated period of time (e.g., two weeks).

The second suggestion concerns the personal identification number (PIN) that shareholders create and utilize in order to conduct transactions and obtain information by telephone on their mutual fund accounts. At the present time, some mutual funds permit a PIN to contain as many as eight digits, but most funds appear to allow a maximum of four digits. All else being equal, however, the security afforded by a PIN is considerably greater with an eight-digit number than with a four-digit number, and a fund family that gives its shareholders the option of using up to eight digits for their PINs seems more likely to be characterized as having acted reasonably. When a PIN is not known by an individual who is attempting to gain access to an account, an eight-digit number is a more formidable obstacle than a four-digit number because the likelihood that the PIN can be uncovered by chance declines rapidly with each additional digit. The likelihood that a PIN of a given length will be found by chance is calculated from a basic principle of probability: with multiple events that do not depend on one another, the probability of obtaining all of the events is the product of the probability of each event.[26] The likelihood that, simply by chance, every number in a set of independently occurring numbers will be discovered is thus computed by multiplying the probabilities of all of the numbers.

In applying the preceding principle, two features of PINs are important: every digit in a PIN can be one of ten distinct numbers (e.g., 0 to 9), and the number for each digit can be selected randomly and, hence, without regard to the number for any other digit. The multiple events here (i.e., the numbers used for a PIN) are thus statistically independent, and since each number in a PIN has a probability of 1 in 10 of being chosen, the probability that, on any single attempt, a particular set of numbers will be selected by chance is $(1/10)^8$ in the case of eight numbers and $(1/10)^4$ in the case of four numbers. A person who did not know the numbers in a PIN and who tried to ascertain them by guessing would correctly pick all of the numbers in a four-digit PIN once in 10,000 attempts, but would do so just once in

26. *See* HUBERT M. BLALOCK, JR., SOCIAL STATISTICS 127-129 (2d ed. 1972).

100,000,000 attempts if the PIN contains eight digits. Expressed another way, the likelihood that a PIN can be found through chance is reduced by a factor of ten thousand if the PIN is increased from four digits to eight.

IV. The Societal Context of Law

Unfortunately, the societal context of law is largely disregarded by persons who have been trained in the field of law. This reality is unfortunate because the societal context of law is the foundation of legal philosophy and rules. Law as an institution is socially determined because it, like every societal institution (e.g., religion, the family), must aid in the functioning of society: to the extent that a social institution does not recognize the problems or reflect the values of society, it will either be changed or discarded. Legal doctrine thus supports and promotes the social order.[27]

This point relates to the mutual fund industry. To illustrate, the proportion of marriages terminating in divorce rose steadily in the United States during most of the twentieth century[28] and, as a result, American marriages are characterized by a high level of instability.[29] Indeed, as many as two out of three couples entering their first marriage between 1980 and 1985 may suffer a disruption of their marriage through voluntary separation.[30] The high incidence of marital breakdown has implications for the security of mutual fund accounts jointly owned by a wife and husband. Fund families may have frequently redeemed shares in such accounts in response to a telephonic request from one of the account owners without realizing that the owners were separating (or had already separated), and that the non-requesting spouse was unaware of the redemption and would be deprived of the proceeds from it.

Is a fund family likely to be liable to the non-requesting spouse when the latter, in completing the account application form and open-

---

27. *See* Larry D. Barnett, Legal Construct, Social Concept (1993).

28. *See* Robert Schoen et al., *Marriage and Divorce in Twentieth Century American Cohorts*, 22 Demography 101 (1985).

29. The United States has the highest divorce rate in the world as measured by time period. *See* Joshua R. Goldstein, *The Leveling of Divorce in the United States*, 36 Demography 409, 414 (1999).

30. *See* Teresa Castro Martin & Larry L. Bumpass, *Recent Trends in Marital Disruption*, 26 Demography 37 (1989). For the purposes of this paper, separation is more important than marital dissolution. However, approximately 95 percent of separated couples can be expected to dissolve their marriages. *See id.* at 40.

ing the joint account with the marital partner, authorized telephonic redemptions by either party? The question would seem to have a negative answer in most cases. However, consider the following situation, which was developed from the account registration form currently used by a fund family. A wife and her husband reside (and work) in geographically distant cities and jointly own shares in several funds of a family of investment companies. The account registration form used by the family includes a section permitting the account owners to instruct the fund family to send a duplicate account statement to a named party at an address other than the one designated on the form as the "mailing address". The couple, in registering as joint account owners, specified the residence of one spouse as the "mailing address" and completed the section of the form authorizing a duplicate statement, in which section they entered the name and address of the other spouse. The couple also authorized (as allowed by the form) the redemption of shares by telephone, permitted the wiring of proceeds of redemptions to a designated bank account in the name of just one of the spouses, and complied with the instructions on the form to attach a voided check for the bank account. The check shows that the bank account is in the name of only one of the owners of the fund accounts. Information on the account registration form, moreover, discloses that the address of the bank is in the same city as the "mailing address" specified on the form and that the owner of the bank account resides in the city where the bank is located.

In this situation, the fund family could easily have known that the joint owners do not share a common residence and that the wiring of monies received from a redemption will be to a bank account controlled by just one of the owners. Is the fund family acting reasonably to protect the interests of the joint owner whose name is not on the bank account if it fails to contact the latter prior to processing a telephone request by the other joint owner (i.e., by the person who controls the bank account) to redeem all (or most) of the shares in the jointly owned fund accounts?[31] Assume that the requesting spouse

31. The account registration form on which I am basing the scenario in the text also includes a section labeled "Investor Profile" that requests information on "annual income," "net worth," and "investable assets." To answer each of these questions, the form supplies four categories. For "investable assets," the categories are $5,000-25,000, $25,000-50,000, $50,000-100,000, and more than $100,000. The section also asks whether the investment objective of the account owner(s) is "growth," "income," or "balanced" and whether the "investment experience" of the account owner(s) is "first time," "limited," "moderate," or "extensive." The section asserts that "Federal and state

asks that proceeds of the redemptions be wired to the bank account. The proceeds will therefore be credited to the bank account and available for withdrawal before a duplicate account statement can be delivered by mail to the non-requesting spouse.

No one, of course, can predict with certainty whether the fund family in the preceding hypothetical will be found liable for the loss sustained by the non-requesting spouse. The matter has not, to date, been litigated. However, the Securities and Exchange Commission concluded in 1997 that an investment entity whose shares are jointly owned by a married couple should, for purposes of the Investment Company Act, deem these shares to have just a single beneficial owner.[32] The position of the Commission may indicate that society has begun to react to the weakening of marriage.[33] Legal doctrine may thus be moving in the direction of reinforcing conventional ideals. If so, courts may start to focus on the factors critical to the institution of marriage, including trust,[34] and to hold fund families responsible for a

---

regulations require that we request this information." According to a representative of the fund family, the purpose of the section is to identify individuals who are investing in funds that might be inappropriate for them. Such individuals are contacted by the fund family and given suggestions as to other funds in the family that they might want to consider. However, an account will be opened even though the section is not completed. Assuming a request is made for a redemption in the circumstances hypothesized in the text and the questions in the "Investor Profile" section were answered by the joint owners of the account(s) involved, caution prior to processing the request would seem to be required when the redemption will constitute a significant percentage of "investable assets." In this situation, the fund family may not be exercising reasonable care if it fails to investigate before processing the redemption.

32. *See* Privately Offered Investment Companies, 62 Fed. Reg. 17512, 17518 n.69 (1997).

33. Evidence of such a reaction can be gleaned from surveys of public attitudes. For example, a survey of a national sample of registered voters conducted in 1996 found that fully 75% of respondents agreed "strongly" with the statement that "[t]here is nothing more important to the future of our society than to reweave the bonds of family, marriage, and parental responsibility." An additional 12% agreed "somewhat" with the statement. A different survey of a national sample of registered voters, also conducted in 1996, found that 42% of respondents "might support" the elimination of "no-fault" divorce. A bare majority (52%) opposed such a change. A large proportion of Americans thus appear to harbor serious reservations concerning "no-fault" divorce legislation. *See* Public Opinion Online (Roper Center), Accession Nos. 0324589 (question 129) and 0287242 (question 30), *available in* LEXIS, NEWS Library, RPOLL File.

34. Americans are cognizant of the centrality of trust in marriage. A survey conducted in 1994 of a national sample of adults asked interviewees to evaluate the importance of trust in a marriage. Trust was considered "extremely important" by 67% of the respondents and "very important" by 31%. *See* Public Opinion Online (Roper Center), Accession No. 0252755 (question 30), *available in* LEXIS, NEWS Library, RPOLL File.

loss, such as that posited above, in order to favor trust in marital relationships. Even if this hypothesis is incorrect, however, a practical consideration dictates that fund families should move aggressively to minimize losses from unauthorized redemptions: the cost of prevention is likely to be less than the cost of litigation and possible liability for losses. Certainly, computers can be programmed to identify jointly owned accounts that, like the account in the above hypothetical, have an elevated risk of sustaining a sizeable loss from the self-seeking conduct of one account owner. For these accounts, the fund family, before processing a redemption request that exceeds a certain threshold, can attempt to contact the non-requesting account owner by telephone or e-mail to determine if the latter is aware of the requested redemption.[35]

V. CONCLUSION

In closing, the mutual fund industry has become an important component of the financial structure of the United States, and American society will be damaged if the industry experiences a significant loss of trust due to security measures that are unnecessarily lax. In deciding on security measures, therefore, the industry should keep in mind that humans have throughout history suffered serious consequences from a failure to exercise care[36] and that what is at stake involves far more than the industry alone. Just as an individual must act in a manner that takes into account the welfare of relevant groups, a fund or family of funds ought to consider the well being of society.

35. Registered investment companies have seven days in which to redeem shares. *See* 15 U.S.C. 80a-22(e) (1994). They are thus not required to process a redemption request immediately upon its receipt.

36. I am reminded of the adage that "for want of a nail the shoe was lost; for want of a shoe the horse was lost; for want of a horse the rider was lost." *See* MACMILLAN DICTIONARY OF QUOTATIONS 460 (1989).