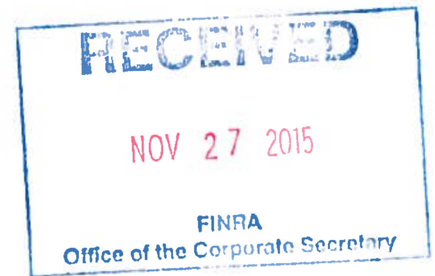


MARTIN B. COWAN
Attorney at law
70 Lovell Road
New Rochelle, NY 10804-2117
Tel: (914) 632 9063

November 24, 2015

Ms. Marcia E. Asquith
Office of the Corporate Secretary
FINRA
1735 K Street
Washington, D.C. 20006-1506

Re: Notice 15-37

Dear Ms. Asquith:

These comments are being submitted in response to the invitation in Notice 15-37, proposing new rule 2165 and an amendment to rule 4512. The effect of these changes would be to permit firms to temporarily suspend distributions of funds to a customer if the firm has a "reasonable belief" that "financial exploitation" of the customer is occurring, or has been attempted or will be attempted. The proposed rule provides for the identification of a "qualified person" at the firm who would have the initial responsibility and authority for making this determination subject to a subsequent internal review of that determination. It would require the firm to make reasonable efforts to identify a "trusted contact person" who would be advised of such a hold, and offer some protection from liability for disclosing private information to the trusted contact person or, if no trusted contact person is available, an immediate family member. It also attempts to offer some protection from liability if the firm declines to suspend distributions. In general, it applies to accounts of investors over the age of 65 but, in some circumstances, will also apply to younger investors. It applies immediately to new accounts, but older accounts will not be covered until a later time.

While the new rule and amendment may be commendable as an initial step in providing some protection against financial exploitation of the elderly, its objective falls too far short of what is reasonable and necessary. But even given that limited objective, it has too many technical deficiencies to accomplish its purported purpose.

The first part of these comments sets forth the reason why a much broader rule is desperately needed and should be adopted. The second part reviews several technical deficiencies and ambiguities that would undermine the proposal's efficacy, even given its much more limited scope.

Part One: Why a Broader Rule is Necessary

To explain why it is so important to have a much broader and more effective rule, it is appropriate to review the nature of the problem in some detail before outlining the steps that need to be taken.

Many of the facts set forth below are well known and mentioned in numerous SEC publications and elsewhere, but they are repeated here for context.

A significant part of these comments refer to IRA accounts because they constitute the largest single category of retirement assets of the elderly[1] and present unique problems[2] for protecting against exploitation. However, to a varying extent, the comments are relevant for all investors, including those under the age of 65.

1. Identifying the Problem

No one is immune from the threat of becoming the victim of a financial predator, but the elderly are especially vulnerable. As we age, the likelihood increases that we will suffer from diminished capacity and lose the ability to protect ourselves adequately from that threat. It is also more likely for the elderly to experience emotional fragility, which contributes to that vulnerability.[3]

---

[1] As of June 30, 2015, the Investment Company Institute estimated that total retirement assets in the US came to $24.8 trillion. Of this amount, IRA accounts, the largest category, hold $7.6 trillion, or close to one third of that total. See https://www.ici.org/research/stats/retirement/ret_15_q2.

[2] Most assets can be protected from fraud by conveying them to trusts of various types. It is also possible to make gifts to adult children. However, none of these methods are available for IRA accounts (including ROTH IRAs). Treasury Regulation Section 1.408-4(a)(2) does not explicitly prohibit a transfer, but subjects the value of an IRA account that is transferred to full taxation at ordinary income rates (which can exceed 50%). This has the practical effect of preventing transfers. Moreover, the laws of every state except Alaska presently prohibit transfers of IRA accounts.

[3] E.g., The Metlife Study of Elder Financial Abuse (June 2011) at p. 22 (http://www.alz.org/facts/overview.asp). See, also, The Interagency Guidance on Privacy Laws and Reporting Financial Abuse of Older Adults :

> "Older adults . . . may be especially vulnerable due to isolation, cognitive decline, physical disability, health problems, and/or the recent loss of a partner, family member, or friend". (https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CCoQFjAAahUKEwi664zdzZDJAhWEox4KHZEPDKo&url=http%3A%2F%2Fwww.sec.gov%2Fnews%2Fpress%2F2013%2Felder-abuse-guidance.pdf&usg=AFQjCNGoJq3CutmLet6lhtV-XbTbP8xGQQ&sig2=shfWum4xPIP11CS9NF5AOg&bvm=bv.107467506,d.dmo&cad=rja)

Peck and Law, in their book, "Alzheimer's and the Law" (ABA Publishing 2013), at pages 297-300 refer to several studies that conclude that, because of changes in the brain that can commence as early as the mid-50s, the elderly lose the ability to discriminate between legitimate requests for financial assistance and fraudulent ones: "These changes in the senior's brain help explain why people that no one ever would have expected are giving money

Recent studies suggest that by age 75, close to 25% of males and 50% of females[4] are already adversely affected by the precursors to Alzheimer's Disease, the most common form of dementia in the elderly.[5] But regardless of these statistics, investors of all ages can be victimized and there is no reason why reasonable steps to protect all of them, regardless of age, should not be adopted, especially where, as in the situations discussed in these comments, the out-of-pocket costs to the institutions for doing so are close to zero.

By the end of 2015, there may be close to $8 trillion dollars in IRA accounts, the largest single category of retirement assets for the elderly.[6] Because of the interplay of the required minimum distribution ("RMD") rules for tax-exempt retirement plans[7] and the long term yields that even conservative investment strategies often produce,[8] these accounts usually reach their

---

away to the Canadian lottery or all these other scams . . .[A]ll of a sudden, many things are believable to them, because of changes in the brain."

[4] Women appear to be twice as vulnerable as men, both to the ravages of Alzheimer's and as targets of financial predators. The Metlife Study of Elder Financial Abuse (June 2011). http://www.alz.org/facts/overview.asp.

[5] The most recent statistics indicate that, by age 85, 36% of the population will have dementia and that, of this group, 95% have Alzheimer's Disease (the remaining 5% includes Parkinson's, strokes and other problems). Two-thirds of the victims are female (suggesting that 24% of males and 48% of females suffer from it by age 85). In all cases, the percentages increase almost exponentially as you go up the age brackets toward 90 and 95. Many observers believe that only half of those who do have it come to the attention of medical authorities, indicating that the real numbers are much worse than these. Finally, recent studies indicate that cognitive impairment actually starts up to 10 or even 20 years before changes in behavior and problems with memory become apparent and Alzheimer's is specifically diagnosed. (See, e.g., http://www.alz.org/facts/overview.asp.) Accordingly, by age 75 or perhaps even earlier, if these studies are correct, a significant percentage of the population will already have begun to suffer a degradation of mental capacities.

[6] As of June 30, 2015, the Investment Company Institute estimated that IRA accounts held $7.6 trillion. See https://www.ici.org/research/stats/retirement/ret_15_q2. This is up from $6.5 trillion as of the end of 2013. http://www.icifactbook.org/fb_ch7.html#snapshot, which extrapolates to a current growth rate of close to another $1 trillion annually. The mere size of this pot of gold in the hands of people who are mentally and emotionally fragile is inevitably going to attract the attention of the wrong parties.

[7] The RMD rules require that, starting at age 70 ½, the owner withdraw a minimum percentage of the account balance each year. That percentage starts at 3.77% the first year and increases a small amount each year thereafter. It does not exceed 5% until age 79, 6% until age 83, 7% until age 86 or 8% until age 89. https://www.irs.gov/.../uniform_**rmd**_wksht.pd. The ICI reports that most IRA account owners over the age of 70½ withdraw only that RMD, and usually withdrew that amount even when the law temporarily permitted them to withdraw less. See https://www.ici.org/ira.

[8] Most investors put a majority of their retirement funds in equities, including mutual funds and ETFs. See, e.g., http://www.icifactbook.org/fb_ch7.html#investors. Over the past 10 years, the average equity yields have exceeded the RMD amounts by significant amounts. For example, as of October 31, 2015, the Dow Jones Total Market Index Fund had a net yield over the past 10 years of 8.07%. Over that same period, the S&P 500 index resulted in a net yield of 7.85%, and the Dow Jones Industrial Average yielded 8.18%. Vanguard's Total Stock Market Index Fund had a return of 8.10%. (For other studies of average yields over extended periods, see http://pages.stern.nyu.edu/~adamodar/New_Home_Page/datafile/histretSP.html_and http://www.stockpickssystem.com/historical-rate-of-return/.) The RMD factor does not exceed the lowest of these numbers, 7.85%, until age 88. Therefore, the typical IRA account balance of an owner who withdraws only the RMD amount has been increasing every year until well past age 85. Moreover, ROTH account owners are not required to withdraw the RMD and, since ROTH withdrawals are tax free, retirees need to withdraw less from ROTH's than from regular IRA accounts to cover the same amount of ordinary day to day living expenses.

maximum values after age 80, just when the frailties of old age start to become significant and the ability of the owners to manage and protect their investments becomes increasingly impaired.

2. Identifying the Vulnerabilities

Possibly as much as 90% of the financial losses to predators is to people known to the victim.[9] This includes caretakers, friends and close relatives. Moreover, it is believed that most losses are not reported. For example, the owner's son may have a gambling habit with large debts, and always be desperate for more money, or a daughter may have a drug addiction with a similar need for acquiring funds at any cost. In these cases, the victim often declines to report the theft because the victim does not want to send a son or daughter or other relative or friend to jail.[10] A more common problem is the trusted caretaker who has access to all of the victim's files and financial statements. The caretaker will quickly learn where the victim keeps a list of passwords and account numbers and how much is in each account. Often, the victim requests the caretaker to assist him or her to manage the financial matters, for example, by helping to log in to a web site or withdraw money from an ATM machine or write out checks or pay a bill with a credit card. Mental problems are not the only reason why the elderly might need and request assistance with such matters. For example, arthritis or other handicaps might make it too difficult for the victim to travel to the bank or use a keyboard, and he will request the caretaker to assist in those activities, either at a computer terminal or an ATM machine. Often, especially once dementia is present, the caretaker can just ask the victim to sign a check payable to the caretaker (or to a friend or relative of the caretaker), with a phony explanation like "it is necessary to pay the electric bill." The victim signs without any understanding of what is involved.

Just as they don't report losses to relatives, victims often do not report thefts by caretakers, either. First, they do not want to admit how gullible they were. Second, they are concerned that if the caretaker is arrested, there will be no one at home to take care of them afterwards. And this assumes that they understand that they were victimized, which is not always the case. Finally, if they do report the loss, law enforcement agencies are usually helpless to do anything about it, anyway.

Accordingly, it is likely that ROTH accounts grow at even faster rates than these numbers suggest for ordinary IRA accounts.

[9] See, e.g., Peck and Law, "Alzheimer's and the Law: Counseling Clients with Dementia and their Families" (2103), a publication of the Senior Lawyers Division of the American Bar Association. The Metlife Study of Elder Financial Abuse, note 3, *supra*, reports that 51% of the losses are to strangers (not clear if this category includes caretakers) and 34% to friends and relatives.

[10] See http://www.nytimes.com/2015/04/25/your-money/as-cognitivity-slips-financial-skills-are-often-the-first-to-go.html?ref=business&_r=1. The article supports the conclusion that "senior abuse is often committed by a close relative or trusted professional" In one case reported in the newspapers, the thief was a "younger" woman (age 63) who married the victim (age 80) and then promptly emptied his bank accounts and insurance policies and gave the money to her own children.

3. Identifying A Solution

In the area of trust and estate planning, a solution to problems of this sort is to use a "protectors' committee". This is a practice that became common in Europe a long time ago and has become almost standard practice today in the United States.

The idea is to have a group of trusted individuals who are able to monitor the actions of the trustee to make sure that the trustee does not engage in actions that are inappropriate. When circumstances call for it, the monitors can step in and require a trustee to post a bond or file a judicial accounting. In appropriate cases, the monitors may also have the right to veto or disapprove actions of the trustee, or require the trustee to make or not make certain elections. If nothing else works, the committee can even replace the trustee or terminate the trust.

This type of approach, which has proved to work very well to protect the family's interests posthumously, easily works to provide necessary protections of the accounts of the elderly during periods of incapacity or declining competency during their lifetime.[11]

To implement this idea, the owner of the account, while still able to make financial decisions (e.g., when creating the trust initially or signing a will), designates one or more trusted individuals to act as "protectors" or monitors.[12] As noted in more detail, below, more than one may be desirable to make sure that one of the monitors does not himself become the problem. Those monitors would have access to account information and receive periodic statements and notices of significant actions. It is possible to also give them various powers like buying and selling securities or even directing distributions, but that is not necessary to achieve the anti-fraud protection.

What is necessary in the current context is that the monitors be alerted as soon as possible to important "red flag" events in the account that suggest that inappropriate activities might be occurring. This can include changes in passwords or sign-ins, changes in beneficial interests (either adding or subtracting beneficiaries or changing the percentage interests of each), changes in bank account linkages, changes in e-mail or postal addresses and distributions

---

[11] The NY Times article noted above, in footnote 7, contains this same suggestion:

> "Another financial adviser asks his clients to assemble what he calls a protective tribe, or a handful of people who are willing to step in and assist if and when the need arises. 'The protective tribe is important because senior abuse is often committed by a close relative or trusted professional,' said Jean-Luc Bourdon, a certified public accountant who specializes in financial planning in Santa Barbara, Calif. 'A tribe is needed to have checks and balances.'"

[12] Having diminished mental capacity, even during the early stages of Alzheimer's Disease, does not necessarily disqualify a person from executing legal documents, including wills and trusts. See Peck, "Exploitation and Alzheimer's, 15 Experience Magazine No.2 (ABA Senior Lawyers Division (2015)). Accordingly, they may still be able to indicate the people whom they trust to serve as monitors or protectors.

that are unusual in timing or amount or otherwise atypical.[13] Notices would be sent out electronically, making them virtually instantaneous.

Upon receipt of information that suggests problems, the monitors can take whatever actions they believe necessary. After inquiring into the situation, they might decide to request the assistance of law enforcement or social services. They may attempt to arrange medical examinations. They may try to eliminate a caretaker's access to the account owner, by removing him (or, with the help of the police, the caretaker) to another location. If nothing else works, albeit as a last resort, they can commence a guardianship or conservatorship proceeding to take control of the victim's finances. Or they might be able to conclude that there is nothing amiss, and take no action at all.

It should be noted that these monitors are persons whom the account owner determined are trustworthy when he was still capable of making that determination. By designating them, he also consents to providing them with confidential information about himself; there is no legitimate concern that providing that information to the monitors involves an invasion of privacy, since full consent to that was given up front. In fact, the consent is not intended to be merely permissive; in these circumstances the owner wants that information to go to the monitors and not to be withheld.

From all of the above, the use of monitors to serve as the analog to a protectors' committee has substantial benefits in securing against fraudulent loss, and no discernible downside. Given today's computer technology, the cost of providing alerts and duplicate statements is infinitesimally small.

Nevertheless, when the undersigned attempted to institute this procedure at several major financial institutions (all members of FINRA), he was usually advised that the institution would not undertake to alert third parties, even those designated for the purpose, of information about his personal accounts. In some cases, the institution justified its action based on privacy concerns; in other cases, no justification was proffered.[14]

Mr. Rick Fleming, Investor Advocate at the SEC, in one of his recent talks, spent some time discussing this privacy concern. He explained that if a financial institution suspected something was amiss, it was difficult to determine whom to warn about that. The financial institution could be giving information to someone who should not be getting it, e.g., the son

---

[13] Another list of "red flag" event, many dealing with the actions of caretakers, can be found in the Interagency Guidance on Privacy Laws and Reporting Financial Abuse of Older Adults, note 3, *supra*.

[14] One institution did agree to most of these suggestions, but sent the notices only by regular mail, which arrived more than one week later. If the addressee is out of town for a week or two, it could take close to a month before he would get those notices and realize that there might be fraudulent activities going on in the account. In today's world of electronic commerce, that delay undermined the value of those notices to the point where they may be close to useless. Another institution said it would only send an alert to the account owner and not to anyone else, even if it knew that the account owner had advanced dementia and did not have to ability to comprehend what the alert was trying to alert him about. It was irrelevant to that institution that such an alert is useless.

with the gambling addiction or a sibling with a criminal record. The account owner may have deliberately withheld from that son or other relative information about the existence or size of the IRA account.[15]

But the situation here is different. The account owner has specified individuals that he believes are trustworthy and has consented to the disclosures.[16] He does not want the information to be trapped inside a black hole where his own support team is unable to see what is happening. The disclosures are almost certainly beneficial to the interests of the account owner and privacy concerns should not stand in the way. Actually, it is virtually impossible to perceive any downside to such disclosures, at least when there is more than one monitor involved. The rules on privacy are intended, and should be construed, to protect the individual, not impede that protection.

Of course, there could be some concern that the monitor might become the financial predator, notwithstanding the account owner's trust. But that risk is almost entirely eliminated by having two or three monitors; each would be in a position to observe the actions of the other monitors and take appropriate steps if needed. The proposed rules already recognize that the financial institution may discover evidence that the person to whom it would normally provide information (i.e., the trusted contact person) is in fact engaged in financial abuse and, in those circumstances it can withhold that information notwithstanding the account owner's permission to release it to that individual. That same limitation can still apply even where the account owner has designated multiple monitors in the fashion suggested in these comments. But the use of multiple monitors makes it much less likely that the institution would ever get to that point.

What is sorely needed, then, is a rule that requires all financial institutions to permit account owners—and, as discussed below, not necessarily just those over 65—to specify one or more monitors who would receive copies of all monthly statements, as well as alerts of red flag events, like changes in beneficiaries and especially the termination of a monitor's status, as quickly as technically feasible.[17] To keep costs down and actually improve efficacy, all such statements and notices can and should be delivered electronically.

---

[15] It may well be that the currently proposed changes to the rules are addressed strictly to the situation contemplated by Mr. Fleming, where the institution has to guess whom to tell. It relieves the institutions from fault if it makes a mistake on whom to contact about suspicious activity by designating a trusted contact party in advance. But it does not cover all of the other possibilities, nor does it even require action in this context. Nor does it entail the involvement of one or more trusted individuals to participate in the detection and possibly the prevention of fraudulent activity unless and until the financial institution first reaches a "reasonable belief" that such activity is in fact happening and voluntarily decides to act.

[16] He can also withdraw or change that designation—and consent—at any time that circumstances indicate that the particular monitor is no longer trustworthy.

[17] It could include the right to give one or more of the monitors powers of attorney, although that is a serious step with potential pitfalls. See, e.g., Kerry Peck, "Exploitation and Alzheimer's, 15 Experience Magazine No.2 (ABA Senior Lawyers Division (2015). A monitor could also have the ability to buy and sell securities, although there might need to be certain limitations on the dual role of monitor and account manager, a matter discussed in the text, *infra*.

To make this work effectively, it is important to make sure that the monitors are themselves alerted to the most important red flag of all: any attempt to remove one or more of them from the picture. That would be the first step any financial predator planning to raid the account would take: shrink the black hole horizon and make sure that no third party can see or get information about what is happening inside the account. But if the monitors are alerted to the termination of their ability to oversee what is going on in the account, they will be able to determine whether that termination is itself a preliminary step to a pending financial exploitation. In these times where everything happens in split seconds on a computer, it is essential that that particular notice be given as quickly as possible, i.e., electronically.

That would advance the cause of protecting the accounts of all investors, not just the elderly. Nor is there any downside to such a rule. [18]

Part Two: Technical Issues with Current Proposal

a) Effective date:

To start with, the effective date of the rule grandfathers existing accounts. Older accounts will not be brought within the rule until a date some time, possibly years, from now. There is no justification for that kind of delay. Older accounts need this kind of protection more, not less, than newer accounts. The older accounts are more likely to be held by older individuals already suffering cognitive and physical impairment, or being cared for by caretakers, and they are more likely to have larger balances than brand new accounts. It is those accounts that need this kind of protection now, not later.

The rules should become effective for all accounts no later than 12 months after they are adopted, if not sooner.

b) Too Much Discretion to Ignore Signs of Fraud:

Next, the rule has little teeth. Apart from the requirement to attempt to identify a trusted contact person, the substantive portion of the rule, i.e., to suspend distributions, appears to be within the sole and absolute discretion of the firm. Nor, unless it determines to suspend distributions, is it required to advise either the account owner or the trusted contact

[18] The recent decision in *Federal Trade Commission v. Wyndham Worldwide Corporation*, Memo Op. 14-3514 (3d Cir. 2015) suggests that institutions risk liability for loss under section 45(a) of the Federal Trade Commission Act if they do not take reasonable steps to protect account holders from losses due to breakdowns in cybersecurity. In the current context, given the extremely small cost that would be involved in providing the greatly enhanced protections suggested by these comments, it would seem unreasonable not to do so. However, it is not clear to what extent the rationale of that decision might be applicable in this context.

person of any suspicions it might have that financial exploitation might be occurring. In fact, the way the rule works, there is a disincentive to do anything at all.[19]

There is no way to overemphasize the need to convey suspicions of financial skullduggery to someone who can protect the investor. Overall, it is submitted that a trusted contact person is in a better position to evaluate circumstances that might be viewed as suspicious. The trusted contact person will have personal knowledge of the account owner that no corporate employee or officer will ever acquire. It is not clear how many accounts a qualified person might be charged with supervising, but it would likely be enough that would make it impossible for him to spend much time studying, learning and understanding the patterns, habits and needs of each and every account owner, even with the assistance of computer programs designed to watch for unusual activities.

The discretion to do nothing, notwithstanding a reasonable belief, or even a strong suspicion, of wrongdoing, is not justified.

c) <u>Safe Harbor Probably Not Needed and, If Needed, Probably Not Effective Anyway</u>

The rule purports to provide a safe harbor from liability for breach of privacy restrictions for disclosing account information to the trusted contact person or other person. But that seems to be a gratuitous provision. A person who designates a trusted contact person to receive information from the financial institution is, by signing the form, waiving any privacy rights that would limit giving that trusted contact person the personal information. If there is any doubt, Notice 15-37 indicates that FINRA expects to release a new form for opening accounts, and an express waiver can be included in that document. On the other hand, if the person opening the account does not adequately waive that privacy right, it is dubious that FINRA can do that by fiat, by issuing a rule of this sort. In general, many, if not most, privacy rights are created by state law, and FINRA does not have the authority to override those state laws. On the other hand, the investor may waive those rights, with or without the authorization of FINRA.

If there is doubt about the validity of the waiver, it should be resolved in favor of allowing the institution to provide that information to the trusted contact person, since the purpose is to protect the owner, not damage him, by that release of information.

---

[19] See proposed Rule 2165(b)(1): "A qualified person *<u>may</u>* place a temporary hold . ." on distributions. (*Emphasis added*). This seems to allow the qualified person to decline placing a hold on a distribution even if he has a reasonable belief that financial exploitation is occurring. There is no requirement to withhold distributions regardless of the circumstances. Moreover, there appears to be a built-in disincentive to withhold distributions even if there is a reasonable belief because of a concern that the owner of the account might sue the firm and/or the qualified person, claiming that the belief and consequent suspension of distributions was not reasonable. If, on the other hand, the distribution is not withheld, the risk of such a suit and the liability (and the corresponding legal costs of defense) disappear. Therefore, from the firm's and the qualified person's viewpoints, it is always safer to do nothing. And if the firm does nothing, it also does not warn either the owner or the trusted contact person of its suspicions of fraudulent activity. Although it may be required to report it to law enforcement agencies, those agencies usually are unable to react with sufficient speed or attention to make a difference.

d) An Account Owner Should Be Allowed To Designate More Than One Trusted Contact Person

The rule only requires that the account owner be giving the opportunity to designate a single trusted contact person. That is insufficient. If the trusted contact person is unavailable or temporarily incapacitated, the financial institution may choose, on its own initiative from within a class of certain close relatives, to whom to provide the information. But the institution has no basis for such a choice. It won't have an ongoing relationship with most, and perhaps, any, of them. The account owner is in a better position to decide on the choice of an alternate trusted contact person. The rule that information would not be given to a trusted contact person if it is suspected that that person might be involved in the questionable activities would still apply to these additional designees. Unless all the monitors are working as co-conspirators (which is unlikely) one of them will realize whether something is amiss.[20]

Any account owner should be permitted to name several monitors (at least three) to avoid the possibility that one of the monitors will become part of the problem rather than part of the solution. If one monitor starts going bad, the other two will be able to see it and take appropriate steps.

Note that if the financial institution suspends distributions, it can only do so for a maximum of 30 days under the proposed rules and, then, it must make the distribution anyway. This stresses the need to permit alerts to more than one trusted contact person. Multiple monitors reduce the problem that might arise if a single monitor were temporarily unavailable for part of all of the suspension period.

e) Different Rules for Those Under Age 65.

While these comments focus primarily on the elderly, there is no reason why the same protections should not be made available to the entire investing public. No one is immune from fraud; advanced age is only a contributing factor. It is even possible for someone under age 65 to have Alzheimer's.[21] The standards for withholding distributions to those under age 65 should be the same as for those over age 65.

---

[20] If there are two and they are closely related somehow, e.g., they are married to each other, or business partners, it is possible that they might be co-conspirators. But even this risk is reduced significantly when a third trusted contact person is involved who is not so related to the other two. If all three are in on the scheme, it may be unlikely that the financial institution will be able to find anyone at all who is not so involved, in which case, no arrangement is going to work out and it is probably time to get law enforcement agencies involved. Having three or more trusted contact persons substantially reduces the chances of that occurring .

[21] Approximately 4 % of the victims are under age 65. http://www.alz.org/facts/overview.asp. In addition, there are persons under age 65 who are partially or wholly incapacitated by strokes, Parkinson's Disease, physical injuries and other ailments.

As proposed rule 2165(a)(1) is currently written, a "Specified Adult" is anyone over age 65. It also includes individuals between 18 and 65, but only if the institution "reasonably believes [that person to have] a mental or physical impairment that renders the individual unable to protect his own interests." It is difficult to understand how an institution that interacts with a customer only on a computer terminal, as is very common today, would be able to know the medical or physical condition of a new customer, or be able to stay current about changes in such a condition in a timely manner.[22] Presumably, the qualified person is not going to invite every customer to dinner one evening a month or so to observe possible changes in medical, mental, or physical condition of the customer, or to be able to evaluate what he observes. The new rule should apply to all account owners over the age of 18. The rule as proposed only requires the institution to do something those over 65 if it has a "reasonable belief" that a fraud has been or is about to be committed. If it has that same reasonable belief about someone who is less than 65—that a financial crime is in progress-- it should take the same actions as in the case of an investor who is age 66. If it believes that a fraud is occurring, it should not be necessary for the institution to have to make additional inquiries about medical conditions of its customer before it acts.

f) Some trusted contact persons should be allowed to have authority to transact business.

Rule 4512(a)(1)(F) provides that the trusted contact person may not be a person "authorized to transact business on behalf of the account". There may be circumstances where this limitation makes sense. For example, there may be a higher risk that a person authorized to transact business on behalf of the account might actually be the potential financial abuser. Moreover, that person already has unlimited access to the information in the account, and giving him or her notice of irregularities may be unnecessary. Alerting a person who already has access to that information may not enhance the protection of the account owner.

However, there are other circumstances where this limitation will impede the objective. As an example, in many families, the spouses exchange durable powers of attorney, to be used at times when one of them is unavailable or incapacitated. Each spouse also gives the other spouse authority to access information about his or her financial accounts and may also include the ability to arrange transactions during either spouse's unavailability or incapacity. Although the second spouse has the authority to access the account and discover what is going on, it is also common for the second spouse not to do that on a regular basis, but only when necessary, or perhaps at specified times, like once a year. Unlike the outside investment advisor who may pay attention to the account frequently, the second spouse may only do that on the rare occasions when the first spouse is unavailable or incapacitated for a long period of time. An alert to that second spouse of some irregularity may be the most effective (and possibly the only) way of stopping a problem in its tracks.

[22] Even the best of physicians have trouble diagnosing mental impairment or the extent to which such impairment makes a patient legally incompetent or unable to manage day to day matters. It is hard to believe that a corporate employee could do better.

This raises the question of what happens if the second spouse is in fact the financial abuser? If the institution suspects that, it can still suspend the distributions and need not send an alert to that second spouse. Under the current rule, it would instead notify another close relative, if one could be found. Moreover, if the suggestion made in these comments to permit the account owner to have more than one trusted contact person, is adopted, this problem becomes moot.

It is suggested that a person should be able to serve as a trusted contact person and also have authority to transact business if that person is a primary beneficiary of the account. That person will have probably the strongest interest in aborting financial misbehavior from the get-go. Alternatively, if there are two or more trusted contact persons, as suggested above, it should suffice that at least one is a person without the authority to transact business. A primary beneficiary should qualify to be a trusted contact person even if he or she has authority to transact business, provided that there is at least one other trusted contact person who does not have that authority. It is submitted that this would provide the necessary safeguards and still allow for a very typical and useful family arrangement with respect to management of family resources.

g) <u>Reasonable Belief</u>

There are also some difficulties about the concept of "reasonable belief". Even a apart from the vagueness of such a standard, it is too strict a standard. Under the rule as proposed, even a strong suspicion of serious wrong-doing would be insufficient to spur any action at all. The rule requires "belief", not mere suspicion, no matter how strong that suspicion may be. The rule requires the qualified person to believe that there is fraudulent activity, not merely suspect it.

Also, the qualified person's conclusion remains subject to an internal review that might or might not back up the qualified person's initial conclusion, leaving him exposed to potential criticism and/or liability. It was noted above that avoiding a threat of litigation creates a disincentive to act; the possibility that the internal review might be critical of the qualified person's actions and that that might adversely affect his potential future with the firm, creates an additional disincentive for any person acting as the "qualified person" from ever reaching a conclusion that there is a reasonable belief, no matter what the suspicious activity might be. Ideally, a qualified person would not let these factors affect his judgment, but we will have to deal with real people, not theoretical ideals, and the actions of real people do not always conform to some preconceived ideal.

In any event, the standard for initiating action and review should be a substantial "suspicion" of potential fraud or abuse, which is a much lower bar to action than a "reasonable belief" that the fraud is actually occurring.

Suspicions are generated by actions that raise red flags. There are many events that may constitute red flags. This includes distributions that are unusual in amount or timing, adding new beneficiaries not obviously related to the owner, or deleting current beneficiaries (especially of a spouse), or changing their percentage shares. Attempts to change bank account linkages or contact information, such as e-mail addresses, may be signs of a problem. There is a list of other warning signs in Interagency Guidance on Privacy Laws and Reporting Financial Abuse of Older Adults.[23] This list includes many examples involving caretakers who make it difficult or impossible to communicate directly with the account owner, or to communicate with him in the absence of that caretaker.

But the most important red flag would be any attempt to delete or change the identity of the trusted contact person or other account monitors. The first step a fraudster is going to do is make sure that no one else can learn of changes in the account or of unusual distributions, so this is probably by itself sufficient to raise a suspicion of fraud.

What the red flag should achieve is that, in and of itself, it may generate a suspicion of fraud that justifies further inquiry. It should not be necessary for the qualified person to first reach a "reasonable belief" that fraud is actually occurring (or occurred) before an inquiry is initiated. If there are two or more unrelated red flags,[24] it should be virtually mandatory for the qualified person to commence that investigation and withhold distributions until, before or after review, it can be concluded that no fraud is pending. For example, if the address to which distribution checks should be mailed is changed at the same time there is the addition of a new beneficiary not related to the account owner, an investigation is probably warranted and no distributions should be made until the original trusted contact person is notified.

In no event should the status of a trusted contact person be terminated until the trusted contact person is notified of that change and a reasonable period of time transpires that permits that trusted contact person to investigate the circumstances.

One red flag may be more important than all the others: if the trusted contact person (or any close relative, attorney or similar individual) notifies the institution that he or she suspects that there is a problem and possible financial fraud, that should be sufficient by itself to hold up distributions pending a review.

Again, this does not place an administrative burden on the institutions. In this day of electronic bookkeeping and accounting, the cost of implementing this proposal is insignificant.

---

[23] Interagency Guidance on Privacy Laws and Reporting Financial Abuse of Older Adults, note 3, *supra*, lists 13 separate items, including a number involving caretakers who make it difficult to communicate directly with the account owner.

[24] By "unrelated", it is meant to discount two or more red flags relating to the same incident, like two situations in which a caretaker restricts access to the account owner at a specific meeting with an account representative. By itself, that may or may not create a suspicion. But if this is accompanied by a change in beneficial interest close in time to that event, it will usually be sufficient to raise a suspicion that requires investigation.

h) Privacy

As previously mentioned, the objection sometimes raised about privacy issues is baseless. This is a situation in which the account owner has consented to giving those trusted contact persons or other monitors full information, if not control, over the account. The customer is the ultimate owner of that information and he wants it to be transmitted to the designated third parties. The owner will not designate anyone whom he believes should not get that information. Releasing the information to the account owner's designees will enhance the security of the owner's account, with only a very minimal risk. Privacy restrictions should not be applied in situations where it is very likely to help the owner avoid a financial disaster, and where the possibility of injury is very remote and extremely unlikely. At most, the institution may opt to warn the account owner of the risks of disclosure, but then it must leave it for that owner to decide for himself whether to accept that risk. If the owner knowingly accepts the risk, the financial institution should not attempt to override that decision, except possibly where it is overly clear that circumstances have changed since the owner made that decision and the institution believes that it has clear evidence that disclosure would now be wrong.

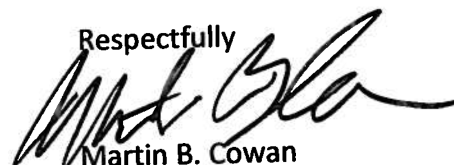
Finally, there is also the problem that, under the proposed rule, an important restriction on the trusted contact person would not apply to the related person who might be contacted when the trusted contact person is unavailable. The limitation, that the trusted contact person may "not be authorized to transact business on behalf of the account", does not apply to the related person contacted by the institution. To the extent that the rule prohibits the designation of a person to serve as the trusted contact person who has authority to transact business on behalf of the account, it makes little sense to not apply that same restriction to providing information to a "close relative" who has that authority.

Accordingly, this comment recommends that further consideration be given to this issue before the final rule is enacted.

Conclusion

Thank you for giving me the opportunity to submit these comments. I will be available to discuss any of these matters with you at any time.

Respectfully



Martin B. Cowan