

WILLIAM H. SORRELL
ATTORNEY GENERAL

SUSANNE YOUNG
DEPUTY ATTORNEY GENERAL

WILLIAM E. GRIFFIN
CHIEF ASST. ATTORNEY
GENERAL



TEL: (802) 828-3171
FAX: (802) 828-2154

STATE OF VERMONT
OFFICE OF THE ATTORNEY GENERAL
109 STATE STREET
MONTPELIER
05609-1001

**Testimony of Vermont Attorney General William H. Sorrell
Before the United States House of Representatives
Committee on Energy and Commerce
Subcommittee on Commerce, Manufacturing, and Trade
May 16, 2013**

Summary

First, I would like to thank the Subcommittee for the opportunity to testify today on a matter of great importance to the Vermont Attorney General's Office and my constituents—indeed to people all over the United States: the tragedy, and the injustice, of fraud perpetrated on the elderly. Citizens in the later years of their life have a right to expect that they will not be at risk from the predations of cross-border and other scammers; and yet financial loss arising from such scams, even the loss of one's life savings, occurs all too often among older people.

Second, I wish to offer the Subcommittee some thoughts, from the State perspective, on what the Federal Government can do to aid in the effort to protect seniors from fraud.¹ Specifically, I have three recommendations to offer the Subcommittee:

- Support research into, and development of, evidence-based, effective programs that go beyond consumer education, to *change consumer behavior* in such a way as to enhance the ability of senior citizens to protect themselves from fraud.
- Support the development of state-level networks, training materials, and protocols to reinforce fraud-preventive behavior by seniors, to identify frauds in real time, and to intervene to prevent consumer losses.

¹ I confine my testimony to the issue of fraud by *strangers*, as distinguished from fraud by people known to seniors, such as family members and caretakers.

- Work with the States to identify third parties, such as wire transfer companies, that, even if not directly complicit in fraud, facilitate the loss of consumer funds, and to take appropriate regulatory and other legal action to stop such facilitation.

The Gravity of the Problem

There are both moral and practical reasons for being concerned about fraud directed at the elderly. For one thing, there is evidence that the incidence of diminished financial capacity increases with age. For another, the older age cohort is growing in America. Moreover, seniors have substantial savings that scammers target, including Social Security, pensions, and veterans and other retirement benefits. These three factors together can be viewed as a “perfect storm”:

Although financial capacity is essential for all community dwelling adults, it is a topic with particularly important implications and urgency for older adults: there is a tremendous and underappreciated “financial capacity problem” posed by our rapidly growing older adult population. Older adults represent that portion of the U.S. population most vulnerable to impairment and loss of financial skills and capacity, as a result of the effects not only of Alzheimer’s Disease and related dementias, but also of normal cognitive aging.

At the same time, older adults hold a disproportionate amount of wealth in the United States. Older adults ages 65 and older currently comprise only 13 percent of the population and 21.4 percent of family households in the United States, but hold 34 percent of the nation’s wealth. This combination of wealth, cognitive decline, and impaired financial capacity represents a tremendous and growing challenge to our society. Given that overall household wealth in the United States in 2009 was estimated at \$53.1 trillion, the amount of wealth currently held in older adult households amounts to a staggering \$18.1 trillion.

With the continued aging of our society, and the tidal wave of Alzheimer’s and related dementias building over the next few decades (estimated at 14 million persons in the United States by 2050), both this percentage and overall older adult wealth will only increase, and issues of financial capacity in elders will become ever more prevalent and urgent. These changing circumstances also provide an opportunity for rethinking how we as a society plan for the future, and how clinicians, social services providers, lawyers, and financial industry professionals can best serve the aging population.²

² “Daniel C. Marson & Charles P. Sabatino, “Financial Capacity in an Aging Society,” in *Generations* (Journal of the American Society on Aging), vol. 36, no. 2 (Summer 2012).

Types of Fraud that Impact Seniors

Some fraudulent practices specifically target older consumers, such as cross-border “grandparent scams.” Others may disproportionately target seniors, such as door-to-door paving and other home improvement scams, or the misuse of names like “Publishers Clearing House” by unrelated companies. Still others may not target seniors more than other people but still affect them seriously. Among the most serious scams we have seen in Vermont are these³:

- **“The grandparent scam.”** An older consumer receives a telephone call from a person who sounds like her grandson; he says he is in trouble and needs money wired to him immediately. Often the story is that the grandson has been in a car accident, or has been arrested, in Canada or Mexico, and needs funds for medical care, bail, or car repairs; the caller will often ask that “his parents” not be contacted. But the call is not from the consumer’s grandson; it is from a scammer. And once the grandparent sends money, the scammer will probably call back and ask for more.
- **Lottery scams.** A consumer receives a call stating that he has won a lottery or sweepstakes or qualified for a government grant but must send money, usually by wire transfer, to cover “fees,” “taxes,” or other charges. But in fact, the lottery/sweepstakes/grant does not exist, the consumer has not won anything, and the money is being sent to a scammer.
- **“Nigerian scams.”** A consumer receives an email stating that a wealthy person has died—often in Africa—and that someone in the U.S. is needed to safeguard the deceased’s money in a bank account. But there is no such wealthy person; this is just a “come on” to lure the consumer to begin sending money—for “fees,” “taxes,” or other charges—to the scammer.
- **“Romance scams.”** An individual is contacted by a stranger, often claiming to be a young person of the opposite sex who wants to strike up a correspondence in the U.S. The stranger expresses an interest in being a “pen pal” and perhaps talks about wanting to come to America to go to school or to meet the other person. Sooner or later there is a heartfelt request for money—to replace a lost airplane ticket, to pay medical bills after a sudden accident, or for some other reason. But it’s a scam, and the stranger, if claiming to be a young female, may even be a middle-aged male.

³ All of these types of fraud are described on the Federal Trade Commission’s website. See <http://www.ftc.gov/bcp/edu/pubs/consumer/alerts/alt111.shtm>; <http://www.ftc.gov/opa/2010/11/onlinedating.shtm>; <http://www.ftc.gov/bcp/edu/pubs/consumer/alerts/alt117.shtm>; <http://www.ftc.gov/bcp/edu/pubs/consumer/credit/cre40.shtm>; and <http://www.ftc.gov/bcp/edu/pubs/consumer/products/pro20.shtm>.

- **Counterfeit check scams.** A consumer who is selling an item online or through the newspaper receives a check for *more* than the asking price. Even if the funds, once deposited, are treated by the bank as “available” for withdrawal, the check is still counterfeit—a fact that is not known for some days or weeks. By then, the consumer has sent a refund to the “buyer” for the excess payment, and that money is in the hands of the scammer. (The use of these counterfeit checks overlaps with other scams, including lotteries, internet auctions, and “secret shopper” scams—this last involving the purported hiring of the consumer to report on how a local business is treating its customers. In all of these cases, the consumer receives an “overpayment” and then is asked to send some amount of money back.)
- **Home improvement scams.** Men in a truck arrive at the consumer’s home and say either that some repair is needed (for example, the roof is in bad condition) or that the men have just come from paving a road with left-over asphalt available at a discount. They convince the consumer to agree to have them repair or pave. The price is high, the work often shoddy, and the ultimate cost is nearly always much higher than the original estimate. Payment is demanded immediately, frequently accompanied by intimidating tactics.

In the past ten days, we added two more Vermonters to the rolls of elderly victims of fraud. One was an 83-year-old man with dementia who lost \$8,000 to an investment scam. The other was a 79-year-old woman who paid a total of \$29,000, in a series of wire transfers, to a “romance” scammer in Ghana.

Anti-Fraud Efforts by the Vermont Attorney General’s Office

Although mine is a small office in a small state, the Vermont Attorney General’s Office has been active in seeking out solutions to the problem of fraud on the elderly. Our Consumer Assistance Program in Burlington promptly processes consumer complaints and makes appropriate referrals to law enforcement attorneys in Montpelier, as well as “riding circuit” to speak at meetings of senior citizens on consumer protection issues. Last year, we chaired a broad-based working group to look into and make recommendations to the Vermont Legislature

on enhancements to Vermont's consumer laws to protect seniors.⁴ Out of that initiative, a protocol is being developed by which my staff will be continuously available to speak with consumers in real time who are identified by local bank personnel as withdrawing cash potentially to send to a scammer.

My staff also participated in the initial convening of experts at Stanford University's Center for Longevity in 2009, to examine the nature of financial fraud, the conditions that make people susceptible to fraud, and potential solutions to the problem.⁵ And Vermont led the first multistate investigations of "fraud-induced wire transfers," which resulted in legal settlements with Western Union and MoneyGram in 2005 and 2008, respectively.⁶

Yet more needs to be done. Cross-border fraud employing Voice over Internet Protocol and untraceable cell phones to telemarket seniors, and anonymous, high-volume emails to target them on the Internet, continue to plague seniors everywhere. Unfortunately, the States do not have the means to pursue scammers in other countries nor, even if we could do so, would we or any combination of governmental entities be able to significantly diminish, through direct pursuit of the scammers, the tide of fraud sweeping in from Nigeria and its West African neighbors,

⁴ See Report to the Vermont Legislature of the Working Group on Protecting Older Consumers (Jan. 2013), <http://www.atg.state.vt.us/assets/files/2013%20Working%20Group%20Report%20on%20Protecting%20Older%20Consumers.pdf>.

⁵ The AARP Foundation and the Stanford Center on Longevity co-sponsored a summit conference in October 2009 on financial fraud crimes, which brought together experts from the fields of social and cognitive psychology, neuropsychology, behavioral economics and communications, federal and state law enforcement, AARP and FINRA. See Stanford Center on Longevity, "Combating Financial Fraud," <http://longevity3.stanford.edu/financial-security-2/combating-financial-fraud/>.

⁶ For information on subsequent settlements with MoneyGram by federal authorities, see Federal Trade Commission, "MoneyGram to Pay \$18 Million to Settle FTC Charges That it Allowed its Money Transfer System To Be Used for Fraud" (Oct. 20, 2009), <http://www.ftc.gov/opa/2009/10/moneygram.shtm>, and U.S. Dept. of Justice, "Moneygram International Inc. Admits Anti-Money Laundering and Wire Fraud Violations, Forfeits \$100 Million in Deferred Prosecution" (Nov. 9, 2012), <http://www.justice.gov/opa/pr/2012/November/12-crm-1336.html>.

from Jamaica and the United Kingdom, from Spain and Costa Rica, and from a host of other countries, including some parts of the United States.

We need to be creative. We need to evaluate the success of our efforts and adjust in the direction of what works. We need to go beyond consumer brochures, posters, and media outreach—unless specific variants on those strategies can be shown to be both effective in changing behavior and financially sustainable. We need to pool the ideas of our best and most experienced experts. We need to forge working partnerships between Federal and State governments. And we need to be successful; we owe no less to our parents and, as we and future generations age, to ourselves and our children.

Recommendations

Here is what I would recommend to you today.

1. *Support research into, and development of, evidence-based, effective programs that go beyond consumer education, to change consumer behavior.* One of the most common governmental responses to fraud is to undertake to educate consumers, through the familiar vehicles of brochures, posters, broadcast media, the Internet, and in-person presentations. However, it is unclear how well these methods actually work to prevent fraud. In fact, the appropriate measure of success in programs of this type should not be, as is often the case, how many consumers were exposed to the message, but rather *whether consumers' behavior has changed, and for how long.* The important questions to ask are: As the result of the particular information-based initiative, are otherwise vulnerable consumers now likely to resist the lottery pitch, or the grandparent scam, or the romance scam; and how long will this change in behavior last? The latter question is as important as the former, because the shorter the fraud-preventive effect, the more costly the initiative is, given the need to reinforce the message.

For example, there is evidence that peer-to-peer counseling (senior volunteers calling other seniors and presenting anti-fraud messages) can reduce potential victims' responsiveness to fraud by "almost 33 percent even after a 4-week delay."⁷ However, that left over 30 percent of the consumers vulnerable to being defrauded again,⁸ and the proven duration of the preventive effect of the messaging would still require frequent reinforcement—so frequent as to be financially impracticable. This is not to say that such approaches cannot be refined and made both more sweeping in their coverage and more long-lasting; but absent research to show that this can be done, it is reasonable to question the efficacy of consumer education, or at least of consumer education alone.

What is needed is a concerted effort to identify ways of changing consumer behavior to maximize self-protection, if such ways exist. Anecdotal evidence does suggest that this will be a challenge, for several reasons. These reasons include the logistical difficulty of reaching most seniors; for many individuals, linguistic or psychological limitations on the capacity to comprehend and then act on anti-fraud messaging; and the reality that when consumers (of any age) are "hooked" on the lure of a supposed lottery prize or the fear of not sending money to rescue a "grandson" from catastrophe, it can be extremely difficult to persuade them that the whole thing is a sham.

In any event, the Federal Government could greatly assist in the effort to develop evidence-based approaches to this problem by providing modest financial support for the work of experts in the field, including continuation of the kind of interdisciplinary exchange that took

⁷ Melodye Kleinman, National Telemarketing Victim Call Center, and Gerri Walsh, FINRA Investor Education Foundation, "National Telemarketing Call Center, Using Peer Mentors to Fight Fraud," http://fraudresearchcenter.org/wp-content/uploads/2011/11/RCPFF_Prevention_Walsh-Kleinman_11.03.11.pdf.

⁸ *See id.*

place at Stanford University in 2009, as well as research at academic institutions and agencies such as the National Institute of Mental Health.

2. *Support the development of state-level networks, training materials, and protocols.*

One approach beyond augmenting consumer self-protection is the development of state or local networks of people who come into professional contact with seniors every day, and who could, if trained and motivated, serve to reinforce fraud-preventive behavior by seniors, identify frauds in real time, and intervene to prevent consumer losses. Candidates for membership in such networks are those who work for local area agencies on aging, senior centers, Meals on Wheels programs, senior housing complexes, nursing homes, home health agencies, medical offices, court systems, programs for persons with disabilities, Social Security Administration offices, and banks, to name a few. Such a system could employ the Coordinated Community Response Model supported in Vermont and elsewhere by the U.S. Department of Justice Office on Violence Against Women in combating domestic and sexual violence.

These are the people who can be trained to spot fraud-in-process—in the senior citizen who mentions a recent telemarketing call from a “grandchild” seeking money, or from a supposed romantic figure on the other side of the world; in the senior who appears excited over expected lottery winnings; in the senior who plans to withdraw thousands of dollars to send to a stranger. These are the people who can be trained to counsel, or to make an appropriate referral, when one of these potential victims arrives at a local senior center, or goes to a doctor’s office, or visits a bank. Comparable training should also be made available to the families of seniors who want to understand better the financial risks that their older relatives confront.

Accompanying the creation of such networks is the need for materials for use in training members of these networks (or in training trainers), and protocols to facilitate appropriate referrals and interventions. With a modest expenditure, Federal, State and private-sector experts could be underwritten to develop such materials and protocols—essentially “programs in a box” to be used, or used as a starting point, in every State.

3. *Work with the States to identify third-party facilitators and take appropriate regulatory and other legal action to stop such facilitation.* Perhaps the most effective approach to reducing fraud directed at the elderly involves something other than relying on seniors to protect themselves, or on professionals in the community to monitor and intervene. It involves instead the identification of third parties, often legitimate businesses, that unwittingly—or sometimes with knowledge—provide the means necessary for scammers to defraud consumers.

The focus on essential third parties has been successful in other arenas. For example, confronted with the decades-long problem of unauthorized charges on consumers’ landline telephone bills (a practice known as cramming), the Vermont Legislature in 2011 enacted an outright ban on most third-party charges to phone bills and eliminated cramming almost overnight.

A similar situation exists with respect to cross-border fraud targeting the elderly. A substantial amount of this fraud involves convincing consumers to *wire* money—typically large amounts of money—to scammers located in other countries or in certain high-risk states. Wire transfers can be picked up almost immediately in any of hundreds or thousands of locations with minimal scrutiny, and thus afford scammers an ideal conduit for the flow of consumer monies.

Major wire transfer companies like Western Union and MoneyGram do have their own anti-fraud programs, some of which have been instituted following settlements with the States⁹ or Federal Government, but the problem of fraud-induced wire transfers continues. Extremely high rates of actual fraud have characterized high-risk corridors: for example, a multistate survey showed that over 29 percent of transfers and 58 percent of transferred dollars from the United States to Canada through Western Union in 2002 were the result of fraud (a number that is believed to have been “artificially” low because the sampled transfers included dollar amounts down to \$300); the comparable figure for transfers to Canada of \$1,000 or more through MoneyGram in 2008 was 79 percent, according to the FTC.¹⁰

These figures—indeed, any figure over a small fraction of a percent—are unacceptably high. The banking system would not allow such levels of fraud, nor the credit card system. What is warranted, then, is a regulatory framework designed to restrict high-dollar transfers through high-risk corridors, at least in the absence of an inquiry by the wire transfer company to the consumer as to the legitimacy of the transfer, while permitting funds sent through low-risk corridors or to any destination in lower amounts to flow unimpeded. In addition, legal obstacles should be removed with respect to the sharing of information on vulnerable consumers among wire transfer companies, so that scammers do not simply migrate to another company. The States have a role in regulating wire transfers to minimize fraud, but so does the Federal Government in setting baseline protections for consumers nationally.

⁹ See, on the multistate side, *In re Western Union Financial Services, Inc.* (Wash. Superior Ct., Nov. 10, 2005) (Agreement), and *In re MoneyGram Payment Systems, Inc.* (Wash. Superior Ct., July 2, 2008) (Assurance of Voluntary Compliance).

¹⁰ See *FTC v. MoneyGram International, Inc.*, No. 1:09-cv-06576 (N.D. Ill., Oct. 19, 2009) (Complaint for Injunctive and Other Equitable Relief), para. 27, <http://www.ftc.gov/os/caselist/0623187/091020moneygramcmpt.pdf>.

Conclusion

The States and the Federal Government are necessary partners in the noble cause of protecting the most vulnerable among us from fraud, most especially our senior citizens. The States can bring to the table their ground-level contacts and their experience working directly with their constituents; the Federal authorities can bring to bear their expertise, financial support, and nationwide regulatory authority. Together, we can, and should, work toward the development of evidence-based strategies to change consumer behavior to be more self-protective; to create networks of contacts, materials and protocols for use throughout the country; and to diminish the use of high-risk wire transfers as an easy way for scammers to take grave advantage of the elderly.

We can do these things, and we must.