THE RISE OF FINANCIAL FRAUD: SCAMS NEVER CHANGE *but* DISGUISES DO

BY KIMBERLY BLANTON

February 2012

INTRODUCTION

The incidence of financial fraud in the United States is on the rise.

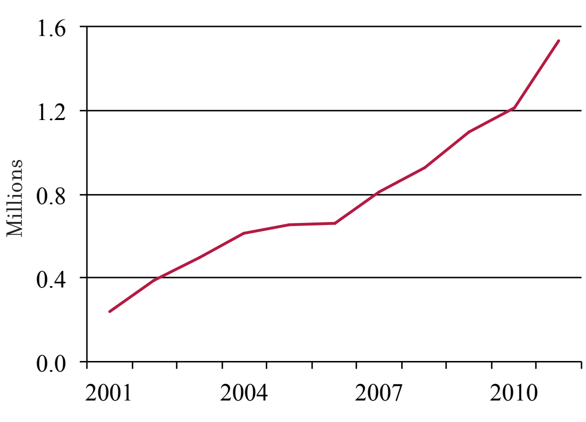
Americans submitted more than 1.5 million complaints about financial and other fraud in 2011 – a 62 percent increase in just three years – according to the Federal Trade Commission's (FTC) annual "Consumer Sentinel Network Data Book" the most comprehensive database of U.S. fraud trends (see Figure 1).

Joe Borg, head of Alabama's securities commission and a leader among state securities regulators, agreed there is a proliferation of fraud, and he largely blames the Internet. His agency had an unprecedented 31-case backlog of criminal trials involving financial fraud in September 2011. "It's not unusual to have 20-25 convictions a year, but when we have 31 backed up – and we're trying them as fast as we can – the trend is up," he said.

Borg ticks off the reasons: "Downturn in the economy. Fear among the public. The idea that the government can't protect them anymore. Medical costs are going through the roof. Those are fears. The Internet is the vehicle. The Internet's a big, big factor."

Neil Power, supervisor of the FBI's Economic Crimes Squad in Boston, said the public is not fully aware of how pervasive fraud is, because only the most prominent cases, such as Bernard L. Madoff's $50 billion Ponzi scheme, are covered by the media. The vast majority of cases fly under the public's radar. "There is a substantial amount of fraud being addressed that's not being covered," he said.

Figure 1. Fraud Complaints Filed by Consumers, 2001-2010, in Millions



Source: Federal Trade Commission (2012).

Many more scammers are never caught by a regulatory system rife with staff shortages and inadequate resources. For example, the Securities and Exchange Commission (SEC) admitted in April 2010 that it has never examined some 3,000 registered U.S. investment advisers, *Investment News* reported. In Canada, only a small percentage of total fraud is reported to law enforcement: one in three Canadians has been targeted by a scammer, yet only 14 percent of fraud attempts

FINANCIAL SECURITY PROJECT at BOSTON COLLEGE

are reported to authorities, according to a 2006 online survey by the Canadian Securities Administrators.

While the Internet has made financial fraud more pervasive, law enforcement said most online scams are not much different than those employed by snake oil salesmen in the 19th century and Florida swamp-land salesmen in the 1960s. Unsuspecting consumers are deceived over and over again with the same schemes, failing to realize that scammers are infinitely creative in making them believe they're offering something new and lucrative.

Scammers may be difficult to recognize, because they constantly alter their disguises. A primary goal of this report is to provide insight into the disguises con men use to perpetrate their standard fraud schemes and to recruit victims who may be retirees, members of the military, college students, the unemployed, homebuyers, investors, low-income families, and others. Cloaked in a new disguise, con men appeal to the individual's weak spot: a desperate shortage of money before payday, a need to earn more than the yield on their certificate of deposit, a need to pay medical bills.

Some con men, for example, may position themselves as a sort of rescue squad, swooping in during a natural or man-made disaster and offering a product or business opportunity that will ameliorate the crisis – and bring untold wealth to investors. Others infiltrate churches where they claim to be doing God's work. Church-based scams are the most common form of what law enforcement call "affinity fraud," which occurs when con men exploit an interest shared by many potential victims, whether a religious belief or country club membership. There are affinity scams against Iranian-Americans, Cubans in Miami, Spanish speakers, Haitian immigrants, and Muslims, among others. Fraudulent subprime mortgage brokers who were immigrants made loans to homeowners who came from their home country and spoke their language.

The sources for this report by the Financial Security Project of the Center for Retirement Research at Boston College included dozens of law enforcement, federal and state financial and insurance regulators, the IRS, financial companies and fraud watchdog groups, as well as publicly available information about civil and criminal cases prosecuted by securities regulators with the federal SEC and state government.

Section 1 provides background on the influences driving the U.S. fraud trend, primarily the Internet, which has enabled scammers to target millions of people in a single keystroke.

Section 2 will identify four basic categories of fraud and describe them. It will also point out the occasional innovation, such as a grim scheme to take advantage of the very old or terminally ill by offering a product that is a twist on legitimate life insurance products.

Section 3 will address the central goal of this report: to reveal six common disguises used successfully by financial schemers to lure unwitting individuals and pursuade them to turn over their money. Awareness of these disguises can help individuals recognize – and steer clear of – fraud.

The final section lists tips to avoid fraud that were provided by law enforcement, regulators, and fraud watchdogs. These tips may help individuals identify suspect behavior, the first step in protecting themselves from becoming one of the millions of victims of financial fraud.

While FTC data reflect the gamut of fraud, this report is limited to fraud involving financial products of all types. This involves any scam that somehow uses or sells a financial product or activity, real or imagined. It may include hedge funds, company stocks, insurance policies, 401(k) and IRA accounts, online brokerage accounts, mortgages, the online payment system PayPal, even income tax filings. Rampant Internet fraud involving such things as consumer coupons, Internet gambling, and sweepstakes is beyond the scope of this report. It also does not address financial products that may be unsuitable, such as subprime mortgages or high-rate credit cards with hidden fees, early payment penalties, steep interest rates, or unfair terms that the typical consumer is unable to decipher.

1. INTERNET FUELS INCREASE IN FRAUD

As the incidence of fraud increases, the dollar amount that victims of all types of fraud reported relinquishing grew sharply, from $343 million in 2002 to $1.5 billion in 2011, the FTC reported.[1] Fraud cost victims $2,267, on average, in 2011.

FTC data are the best available but do not capture the scope of financial-product fraud. The agency tracks only complaints submitted by consumers – and not convictions or civil complaints filed by state securities regulators and federal and state law enforcement officials. The data are compiled from consumer complaints submitted to the FTC by agencies such as the FBI's Crime Complaint Center, the Better Business Bureau (BBB), the U.S. Postal System, the non-profit Identity Theft Assistance Center, which is supported by the financial industry, and the National Fraud Information Center, which is operated by the non-profit advocacy group National Consumers League.

The complaint data shown in Figure 1 fall into the FTC categories of Fraud and Other consumer complaints; a third FTC category – Identity Theft – was excluded. The Fraud category includes debt-collection scams, business opportunities, fraudulent lenders, and advance-fee fraud discussed later in this report. But it also includes non-financial fraud involving health care products and home appliances. The Other category includes misleading real estate practices, false debt collection protection, and deceptive lending, but also auto- and home repair-related complaints.

A former FTC program manager for the Data Book, John Krebs, said the dramatic increase in fraud reflects, in part, that the agency has enlisted more organizations to supply their complaint data; that individuals are becoming more aware of the FTC complaint network; and that consumers are more aware of fraud, especially in the wake of widely publicized credit card fraud at prominent retailers or Madoff's spectacular Ponzi scheme.

FBI and state securities officials confirmed they are prosecuting more financial fraud. They identified three major culprits in the fraud epidemic: the Internet, the 2008 financial market collapse, and the financial insecurity felt by Americans due to the economic slowdown.

There is also a growing consensus that fraud against seniors is increasing, said Andrew Roth, former director of fraud education and outreach for the California Department of Corporations, the state's securities regulator. Aging baby boomers, who have accumulated substantial assets either through inheritance, home equity, or a lifetime of saving for retirement, are ripe for abuse.

"They're a larger and wealthier population than ever," Roth said.

The Internet has been a boon to scammers, who use social networking sites such as Facebook and Twitter to commit fraud. The Web makes it easy to commit fraud from international posts. In one

[1] Dollar losses represent all FTC fraud categories; Figure 1 includes only Fraud and Other complaints.

cutting-edge scam, hackers cracked into individuals' bank, credit card or other accounts and used the account holders' money to carry out transactions or make investments without their authority. In 2008, a Malaysian hacker received a two-year sentence after the FBI charged he had hacked into 60 Americans' investment accounts at nine brokerage firms to buy and inflate the price of a stock he owned, so that he could sell it for a profit.

With the advent of the Internet, "the perpetrators are anyone," said Jason Boone, a researcher for the National White Collar Crime Center in West Virginia. "There are gangs perpetrating crime over the Internet. They might as well give up gun running. They can make money this way."

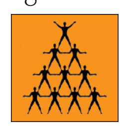
"Phishing" is an old-fashioned scam that once targeted hundreds of people through fliers or the U.S. mail. Today, online scammers phish for millions of prospective victims, sending emails that appear to come from legitimate financial organizations, whether American Express, the IRS, Bank of America Corp. or others. In a typical phishing expedition, a mass email instructs targets to click on a link that directs them to a site that looks legitimate. In fact, these are fake websites, which can deceive individuals into supplying personal financial information, account numbers, passwords, or Social Security numbers.

Economic hardship means more people have less money to risk with shady deals. But economic hardship also makes people more vulnerable – and scammers more desperate and creative – authorities said. Alabama's Borg said the financial-market collapse in 2008 created new potential targets, whether young working professionals distrustful of traditional stock and bond markets, baby boomers panicking about insufficient retirement savings, the unemployed living on the edge, or retirees dissatisfied with the historically low rates they are earning on their assets.

With Americans swimming in debt and earning less to repay it, regulators and consumer advocates report a growing problem with scammers purporting to be debt- or mortgage-resolution firms. These fraudulent firms charge an upfront fee but never deliver the financial service promised.

In a bad economy, "You've got a huge, huge market to tap if you're a con artist," Borg said.

2. FINANCIAL FRAUD: NOTHING NEW UNDER THE SUN



Ponzi scheme operators are by their nature brazen. Even so, Hamilton Alan Bird stood out from the crowd. This was not because he siphoned $24 million from some 360 investors for his hedge fund by promising to nearly double their money in less than a year. Nor was it because he used the money to buy himself a Challenger 600 jet and prime Florida real estate.

What was most brazen about Bird's fraud was that on Sept. 5, 2008 – just hours before a Colorado judge sentenced him to 24 years in prison for a Ponzi scheme – he had convinced investors to put $25,000 into a new scam. Bird was later sentenced to four more years in prison for the second scam, which he had operated while his original criminal case was moving through the courts.

Bird's success demonstrates the gullibility of unsuspecting individual investors, who leap at dubious opportunities to get ahead of the financial game. None of Bird's investors apparently had seen any of the numerous news articles revealing what he was up to.

"That was pretty egregious," said Fred Joseph, who, until the Bird scheme, thought he'd seen it all during 18 years as securities commissioner of Colorado.

Bird used the well-worn tools of his trade to recruit "investors" in a non-existent hedge fund. An array of familiar schemes like these pops up over and over again, year after year. This section identifies and briefly describes four broad categories of these standard frauds. "The types of fraud have not changed," said John Gannon, former senior vice president of the FINRA Investor Education Foundation. "What has changed are the communications tactics used to commit fraud."

Consider perhaps the most famous investment scam of all. In the 1920s, an Italian immigrant named Charles Ponzi operated his scheme out of an office near Boston's City Hall, Mitchell Zuckoff wrote in "Ponzi's Scheme: The True Story of a Financial Legend." Ponzi's purported investment strategy involved archaic "postal coupons" no longer in use. He was so adept at attracting money that Boston media touted his purported financial genius. "WE GUARANTEE YOU 50 PERCENT PROFIT IN 45 DAYS," the *Boston Traveler* blared in a headline about Ponzi's firm. The article went on, "We haven't figured out how they make their enormous profit, but they seem confident of their ability to do so." The basic Ponzi scheme persists today. For example, Madoff adopted Ponzi's core strategy of using new investors' money to pay the high "returns" to early investors that are essential to keep the deception alive.

The financial market collapse in 2008 exposed Madoff, who, like Ponzi, ultimately could not meet his jittery investors' demands that he return their money. The market collapse also exposed the pervasiveness of Ponzi schemes during the economic boom early this decade. An Associated Press analysis of 50 states found that tens of thousands of Ponzi investors "watched more than $16.5 billion disappear like smoke in 2009." There is little doubt the Ponzi scheme will return, cloaked in a new disguise, at a future date.

The following describes the four common categories of financial-product fraud against individuals, according to interviews with law enforcement:

A. All **investment frauds** have one thing in common: they sell something – a company, product, or promised rate of return – that either doesn't exist or will not live up to expectations. The primary categories are:
   - The Ponzi scheme promises extraordinary investment returns that may materialize initially, as long as the perpetrator can bring in new clients. But the scheme collapses when new investors are no longer willing to supply new money to the investment scam to pay off its earlier investors.
   - Pump and dump scams occur when con men send out inflated and inaccurate information about a company's stock that they already own. Their reports hype the company's profits or business prospects with the goal of encouraging naive investors to rush in and buy the stock. When they do, surging demand drives up the price. The fraudster sells his shares at a large profit, leaving defrauded investors holding stock that inevitably collapses in price once investors realize the hype is baseless.
   - Fake or dubious investment companies sell shares, equity stakes, or debt, purportedly backed by a hot new product, technology, or business opportunity. These scammers sometimes go to great lengths to create the appearance the company they are touting is real. In one major Massachusetts case, Secretary of State Francis Galvin reached a settlement with a man who claimed to have special contracts to act as a broker and sell uniforms for a Japanese manufacturer. He then allegedly sold promissory notes to investors who

loaned him money to handle the uniforms. The entire story was fabricated, the SEC said. "There are millions of cases like this," the FBI's Power said.

- High-yield investment fraud has become popular. Con men sell either a bond or a loan and claim the securities have the contradictory characteristics of low risk and high yield. The returns promised on these, as one Canadian regulator put it, are "so high it could not be earned through legal means."

B. **Advance-fee scams** comprise a second category of fraud.

- Debt-settlement scams became pervasive in the recession as consumers struggled to pay credit card debts or carry mortgage balances that exceeded the value of their homes. To solve consumers' problems, fraudsters pose as debt experts or lawyers and offer to negotiate on their behalf with a lender for an affordable payment schedule or reduction in debt. Fraudulent debt negotiators require customers to pay an upfront fee but never handle the problem. Advance-fee scams involving other financial products also exist, but the outcome never varies: the fee is paid and the promised service is never delivered.
- **The notorious Nigerian scam** in which someone receives an email requesting they turn over money or their bank account number is a form of advance-fee fraud, also documented by Zuckoff, in *The New Yorker* magazine: Massachusetts psychotherapist John W. Worley received an email from a Nigerian who purportedly needed help transferring $55 million to the United States. If Worley would only provide money upfront to transfer the money, he would be richly rewarded. He was not. "Advance-fee fraud is an especially durable con," Zuckoff wrote. "In an early variation, the Spanish Prisoner Letter, which dates to the sixteenth century, scammers wrote to English gentry and pleaded for help in freeing a fictitious wealthy countryman who was imprisoned in Spain."

C. **Insurance fraud** typically involves someone staging a fake accident or arson fire to collect on their policies illegally. But fraud is also perpetrated against individuals who buy insurance policies.

- Premium payments are diverted when unscrupulous insurance agents or brokers sell a purported health, auto, home or life-insurance policy and deposit the customer's funds in their personal bank accounts.
- Fabricated policy documents give the fraud target the impression that the coverage is in effect and encourage them to pay the monthly premiums, though no policy exists.
- Legitimate insurance products such as annuities and so-called viatical settlements can serve as valuable options for people near or in retirement. But their complexity itself can also be used to the con man's advantage. In a viatical settlement, for example, the terminally ill, such as AIDs patients or the elderly, are persuaded to assign the death benefits on their life insurance policies to an investor in return for a lump sum to pay their living or medical expenses. Regulators are increasingly alarmed that these products can provide opportunities for con artists to victimize the sick or vulnerable. "That whole area is rife with potential problems," said Massachusetts Secretary of State Galvin.

D. Tax fraud usually involves wealthy taxpayers who fabricate or exaggerate deductions or hide their income illegally in the Caribbean to evade substantial IRS liabilities. But common tax scams victimize low- or middle-income tax filers.

- In one such fraud, tax preparers use false deductions or manipulate a client's income to convince him that he is eligible for a large tax refund; the preparer then extracts a fee from the inflated return, and the tax filer must repay the IRS for taxes owed due to the fraudulent tax return.
- In another case, preparers in Arkansas, New York, and North Carolina made so-called "Refund Anticipation Loans," which charged fees or interest rates in violation of state laws, according to the National Consumer Law Foundation, a Boston consumer organization.

3. SCAMMERS' DISGUISES

All successful con artists achieve the same goal: separating people from their money. But their potential targets can prevent fraud if they recognize scammers' disguises, the dazzling shrouds that hide the same old frauds and deceptions over and over.

"Everything is a rehashing and a redressing of what's come before," said Boone at the National White Collar Crime Center. "The technology changes. The phishing you have today is email but, before the Internet, people were sending out flyers, saying, 'Give us a call and we'll help you make more.' It's become more sophisticated. It's a lot more subtle. They really are the same thing."

So many scams are running all the time, it is impossible to present a comprehensive list of all the disguises used. The following are six common ones. To illustrate each disguise, two sample cases are described.

A. The Rescue Squad.

Scammers sensing an opportunity often sweep in during the weeks after a national disaster, whether the Sept. 11 terrorist attacks, Hurricane Katrina, or an environmental catastrophe such as the BP oil spill in the Gulf of Mexico. With all eyes trained on the disaster, the Rescue Squad presents a solution they claim will put untold profits into the pockets of individuals. In another variation, they devise products that offer a miracle solution to a prominent commercial or technical problem that is frequently in the news and familiar to most.

Con men "follow the headlines," said Tanya Solov, director of the Illinois securities department. Sometimes even the problem they are urgently trying to solve is a fabrication: Solov recalled an Illinois investigation into a company in the 1990s that tried to sell investors on using ostrich feathers to clean compact discs. "I didn't even know they needed cleaning," she said.

- **Red Flag**: any financial offer that comes on the heels of catastrophe and attempts to capitalize on that event is suspect.
- **Financial Products Involved**: company stock, Pay Pal, loans, private placements in company stock or debt and other investment vehicles.
- **Case 1: Gulf Oil Cleanup**: In June 2010, two months after the explosion on the Gulf oil rig, the *Press-Register* in Mobile, Alabama, reported that executives of a Chicago-area company,

InfrAegis Inc., were in town pitching investors on a "bacterial consortium" that could eliminate the oil pouring into the Gulf of Mexico. That same month, the Illinois Secretary of State was ordering InfrAegis to halt the sale of unregistered securities in a wireless company. In July, the Alabama Securities Commission followed with an order that InfrAegis executives halt sales of securities in the oil-cleanup company, which regulators said were not registered. The SEC in October filed charges that the company defrauded investors out of $20 million for purported sales of homeland-security products. InfrAegis did not return several calls seeking a comment to its headquarters in suburban Chicago.

- **Case 2: Salvation Army**: Days after Hurricane Katrina slammed the Gulf Coast, Texas brothers Steven and Bartholomew Stephens registered a website, salvationarmy*online*.org [italics added], purporting to take in donations for hurricane victims; the Salvation Army's actual website is salvationarmy.org. The fake website accepted donations through an online PayPal account that diverted them to the Stephens' bank accounts. More than 250 people sent in $48,000 before the fraud was discovered, according to the U.S. Attorney's Office in Texas. The brothers began serving prison sentences in November 2007.

B. The Problem Solver.

Con men are experts in the psychology of their prey. The Problem Solver targets individuals in financial distress who feel they have nowhere to turn for help. Fraud against those down on their luck or wading in debt increased during the recession, law enforcement said. Senator Charles Schumer, a New York Democrat, felt the problem was so pervasive that he sent out a public alert about automated "robocalls" by scammers charging an up-front fee to negotiate a lower interest rate on a credit card, which "consumers can do on their own for free."

- **Red Flag:** Problem Solvers offer simple solutions to what their victims should know are complex financial problems, having tried, and failed, to remedy the problem themselves. Yet, they want to believe a scammer who promises to take on their problem can solve it.
- **Financial Products Involved:** Credit cards, mortgages, pay-day loans, insurance.
- **Case 1: Debt Resolution scams** were common during the recession. An Alabama judge in February 2010 permanently shut down what that state's Attorney General called "one of the largest debt settlement schemes in the nation" against 15,000 Americans mired in credit card and personal debts. The Alabama Securities Commission, which had requested the action, said the company promised "superior results" and convinced customers to pay millions in upfront fees and then stop paying their debts, forcing the credit card company or other lenders to settle. This plan failed and the customers' credit ratings were ruined.
- **Case 2: Online payday loans:** Payday loan stores, a common site on street corners in low-income neighborhoods, now operate on the Internet. Payday loans, which charge high fees and interest rates for short-term loans, can be useful, but they can also trap borrowers into falling even further behind on their bills. Online payday loan companies are especially dangerous, regulators said, because customers that supply bank account or credit card numbers are at the mercy of potential scammers who have authority to withdraw money from their accounts. 500FastCash is one of numerous online payday lenders that have sparked hundreds of complaints, the BBB warns on its website. BBB staff said they went to Oklahoma to talk

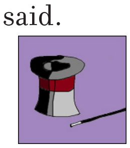
to the company and found the Casino and Smoke Shop operated by the Modoc Indian Tribe; the tribe said it was unaware of 500FastCash. The Bureau reported some FastCash customers never received their loans, while others continued to receive unauthorized charges to their credit cards after the loans were paid. Attempts by the Financial Security Project to contact the company for a comment were unsuccessful. A customer service representative confirmed the headquarters was in Miami, Okla.; the company did not return messages seeking comment.

C. The Senior Specialist.

Senior Specialists target victims for no other reason than that they're one of more than 40 million Americans over the age of 65 and, therefore, more likely to have money in the bank or equity in their home. Fraud against seniors took off in the late 1990s, experts said. This prompted California regulators to institute a Seniors Against Investment Fraud program in 2005, and the North American Securities Administrators Association alerted seniors to check credentials for people they do business with.

- **Red Flag:** Fraudulent senior specialists claim to possess special training to help seniors deal with their specific problems. Knowing seniors tend to be risk-averse, they ease seniors' fears by promising the financial products they are peddling are "low-risk" or "no-risk." Or they lure them with promises of larger returns than they currently earn from their traditional stocks, municipal bonds, and certificates of deposit.
- **Financial Products Involved:** Stocks, bonds, private placements in company stock or debt, insurance, high-yield investments.
- **Case 1: Financial adviser**: Jeffrey Gordon Butler's clients in southern California trusted him. After all, he had helped them prepare their wills and trusts. When he said he had found an investment that paid 12 percent, 124 clients turned over some $11 million. It was a Ponzi scheme, and their savings vanished. "We fell for it," Ann Poor, a retired school teacher who lost more than $300,000, told *The Orange County Register*. Butler, who is serving 90 years in prison, used a typical Ponzi ploy to keep investors in the game: new investors supplied cash to pay off earlier investors and keep them happy. "For a while, we were getting $740 a month in interest, and that was real good. So, we went ahead and gave him most of the rest of our money," Poor said.
- **Case 2: Investment advisor**: In October 2010, Stephen Clifford was sentenced to prison time related to a $3 million scheme in which the SEC alleges he acted as an investment advisor for seniors, including one woman who wanted to give money to her children. He promised the money would earn about 7 percent annually – better than the return from traditional markets but not so high that it raised red flags. Clifford posed as a financial adviser to seniors, "assuring them that he would select appropriate securities for their financial needs and tolerance for risk," the SEC said.

D. The Magician.



The Magician often tantalizes customers with a free lunch, steak dinner or educational seminar. If he can persuade them to attend, he can personally charm them with offers to perform magic, effectively giving something for nothing.

- **Red Flag:** A high return, at no risk to the senior, is impossible in the investment world. But the Magician lures his prey using terms such as "minimum guaranteed return," "triple your investment," "profits guaranteed," or "can't lose any money."
- **Financial Products Involved:** Company stock, private equity or debt placements, high-yield investments.
- **Case 1: "Outlandish" returns:** Some 40,000 people in more than 120 countries believed Nicolas Smirnow's sales pitch on his website, "Path to Prosperity, or "P 2 P," and lost more than $70 million in the global fraud, according to the complaint filed by the U.S. Attorney's Office in Southern Illinois. Authorities said Smirnow allowed customers to select their investment plan: a seven-day plan supposedly earned 546 percent; a 60-day plan earned 720 percent. A resident of the Philippines, Smirnow, whom authorities said operated out of Canada and the Philippines, and whose website was based in the Netherlands, could not be located to comment on the allegations.
- **Case 2: "Unique investment strategy:"** An $8 billion fraud case filed against Texas financier R. Allen Stanford in February 2009 was one of the most highly publicized to emerge from the fallout of the financial market collapse. The SEC said Stanford touted a "unique investment strategy" to sell high-yield certificates of deposit and claimed he earned fantastic returns, even though clients were losing money; the trial began in January. Stanford has fiercely denied the SEC charges and filed a lawsuit accusing the agency of using "illegal tactics" in pursuing its case.

E. God's Messenger.

Fraud inside religious organizations generated publicity in the late 1990s and persists today. Scammers see church pews lined with potential victims, and they exploit a unique vulnerability shared by congregants: trust. God's Messenger often shows up in the guise of a minister or friendly fellow or congregant who has stumbled onto a fabulous deal. "People tend to not do the due diligence," when they meet a scammer at church, Keith Woodwell, director of the Utah Division of Securities, said. The duped individual mistakenly thinks, "I can trust him."

- **Red Flag**: Anyone selling financial products at a place of worship may be suspect. Scammers often co-opt congregants to describe how much money they've made, which gives legitimacy to the scheme.
- **Financial Products Involved**: All products.
- **Case 1: High-Level Fraud**: A former bishop at the Church of Jesus Christ of the Latter Day Saints, Shawn R. Merriman, pleaded guilty to operating a more than $17 million Ponzi scheme in which he used his rank within the church to take in Mormons, news reports said. Authorities said he operated the scheme for 15 years, promising more than 100 investors in Colorado, Minnesota and Utah returns of 7 percent to 20 percent every year on stocks and bonds he purchased on their behalf. He never bought the securities and instead used their money to buy an Idaho cabin, classic cars, including an Aston Martin, and religious art, including two Rembrandts, which he exhibited at LDS Centers in Denver and at the Museum of Church History and Art in Salt Lake City.

- **Case 2: Rewards for "God's Work:"** An Arizona judge in 2006 sentenced two former top officials of the Baptist Foundation of Arizona for a scam that mixed religion and money. When *The Washington Post* reported the scam, which tricked some 11,000 investors out of $585 million, it was one of the largest church-based scams in history. Salesmen quoted the Bible to persuade donors to invest in the foundation; they would, they said, receive extraordinary financial rewards for doing "God's work," such as building churches and retirement homes. William Pierre Crotts, the foundation's president, was sentenced to eight years, and Thomas Dale Grabinski, former chief legal counsel, received six years.

F. The Confidant.

When securities regulators discuss the serious matter of financial fraud, an inside joke invariably comes up. Why, they ask, don't fraud victims wonder why someone who has found the secret to untold wealth is willing to share it? That paradox explains why the Confidant's tactic is so successful: con men who claim to share a secret are transmitting the message that their unwitting victim is special.

- **Red Flag:** The Confidant often asks his victim not to tell anyone else about their exclusive arrangement. He or she may say the victim is lucky to be a member of an exclusive club or a group of people capable of understanding the offer, or possessing enough money to benefit from it.
- **Financial Products Involved:** Private placements of stocks or bonds, debt resolution, insurance, bank notes.
- **Case 1: "Turn Debt into Wealth:"** In Massachusetts, a "personal coach" told a prospective client he could "turn debt into wealth." Darin Floyd Beal recommended that a 59-year-old client extract $100,000 in equity from her home to make this profitable investment, according to an April 2009 complaint filed by the Massachusetts Securities Division, which suspended his broker's license. In an email, Beal created the air of exclusivity: the deal "only allows what are called 'accredited investors' so you have to have deep pockets to invest in them. So what I am proposing is that you invest the money through me and I will do the investing for you," the complaint said. In April 2009, the Massachusetts securities division ordered Beal to cease operations in the state; the case is now settled, the division said. An unidentified family member at Beal's Utah residence said he settled the case but "didn't admit to the allegations;" Beal did not return a message left for him personally.
- **Case 2: Elite Banks:** The Confidant is master of the so-called prime bank scheme, which became popular in the late 1990s. The scheme lured investors to deposit their money in secretive, exclusive overseas banks purportedly doing business with Saudi sheiks or the Rothschilds. In one Texas case, convicted scammers promised 30 percent *per month*, guaranteed by a major European bank or Caribbean insurer, according to the SEC. "Because there was no real investment, some investors received partial, 'Ponzi' payments, and others received nothing," the SEC said. The perpetrators used the money to buy houses, cars and boats, the agency said.

TIPS FOR AVOIDING SCAMS

Fraud schemes share similar warning signs. Potential victims who recognize them may be prompted to investigate an offer for a financial product before buying it, contact regulators, or walk away. Boston College's Financial Security Project compiled a list of 10 red flags based on tips provided by securities regulators, attorneys general and anti-fraud watchdogs around the country.

Potentially fraudulent deals:

1. **Look too good to be true.** Scam products or investments usually appear far more lucrative than standard products on the market. Click here for more information from Finra.
2. **Offer a high or "guaranteed" return at "no risk" to the investor**. This is virtually impossible since the riskiest investments produce the biggest rewards – and failure rates – and safe investments typically offer predictable but modest rewards. Check out a broker.
3. **Require an urgent response** or cash payment. Offers by high-pressure salesmen should be avoided altogether. Responsible financial advisors do not rush prospective clients into hasty, and regrettable, decisions.
4. **Charge a steep upfront fee** in return for the promise of making more money at some unspecified date in the future. An honest contractor will ask you not to pay for a kitchen renovation until the work is done – ditto for financial products.
5. **Suggest recipients do not tell family members** or friends about the offer. Ask yourself, what is this person trying to hide? Probably a fraud.
6. **Lure prospective investors with a "free lunch."** Con men set these up to make their fraudulent pitches in person and increase their chances of success. Watch "Tricks of the Trade" by *NBC*'s Dateline. Remember, there is no such thing as a "free lunch."
7. **Come unsolicited over the Internet, are of unknown origin**, or come from overseas or from an individual or company that is in any way unusual or suspect. Anyone can hack a computer and send out an email message – and con men often do.
8. **Instill fear** that a failure to act would be very costly. Coercion is not used as a tactic by someone giving sound financial advice.
9. **Resist being questioned or checked out further**. Con men flee when someone starts asking serious and detailed questions. Watch Chapter 1 of "Fraud Scene Investigator" to learn more. Legitimate brokers or advisers, on the other hand, will patiently answer questions.
10. **Are so complex that it is difficult or impossible to understand**. Scammers often dazzle or intimidate their targets with their superior knowledge of finance or with complex mathematical explanations. A good rule for any financial transaction: if you don't understand it, don't do it.

The Center for Retirement Research thanks AARP, Invesco℠, LPL Financial, Mercer, MetLife, MFS Investment Management, National Reverse Mortgage Lenders Association, Prudential Financial, Putnam Investments, State Street, TIAA-CREF Institute, T. Rowe Price, and USAA for support of this project.