Financial Abuse

New Trends in Financial Abuse and Identity Theft

by Dana Shilling

Frauds and scams have been part of the human landscape from time immemorial. There always has been and always will be a minority of people who are willing to cheat, defraud, and harm others to make a profit. Dana Shilling's voice is among the loudest of those who warn about such dishonest practices and advocate for its victims. In this article, she offers concise information and recommendations to combat some of the more common financial improprieties and fraudulent schemes that have emerged during the digital age, especially the ones that impact the vulnerable elderly.

Some forms of fraud and financial exploitation are decades or even centuries old; some are newer, relying on computers and the Internet. This article discusses the newly identified trends of deed forgery and manipulation of automatic debits from accounts, as well as identity theft. To assist the vulnerable, there are advocates on behalf of potential victims, such as the CFPB, and Fidelity Investments has launched a program to train financial advisers to offer better service to senior-citizen clients.

REAL ESTATE SCAMS

At one time, establishing the ownership of real estate required research in dusty official record books. The computerization of those records has made it easier for legitimate inquiries to be pursued digitally and made it possible to access the records online without having to travel to the recording office. The downside is that digital information can be manipulated for fraudulent purposes.

Deed Forgery

A new financial threat involves hacking online records to forge property deeds, sell the properties, and steal the proceeds. Four arrests were made in the case of retired nurse and property investor Sybil Patrick, age 79. When

Patrick went to one of her properties to do some gardening, the superintendent of the building next door asked her why she was working on a house she had sold. Upon investigation, Patrick found that, without her knowledge or consent, the property had been sold for $750,000, and the thieves kept the proceeds. (Laura Kusisto, *Latest Cyberthreat: Stealing Your House*, WSJ.com, Dec. 8, 2015, *available at* www.WSJ.com/articles/Latest-Cyberthreat-Stealing-Your-House-1449622684 at 3.) Three people were charged with grand larceny for defrauding Patrick; two pleaded guilty, while one was arraigned in late 2015 and pleaded not guilty.

To increase transparency in real estate transactions, many public documents (deeds, mortgages, etc.) have been made available online; these show the owners' signatures, addresses, and mortgage amount, as well as the size of liens on the property. Manhattan Executive Assistant District Attorney David Szuchman says that this laudable attempt at making information readily available became "one-stop shopping for fraud," which has become epidemic in Manhattan. The swindlers get a quick sale by underpricing the property, pressuring innocent buyers to close the deal quickly, and then using the publicly available information to forge a deed transferring the property to new owners. New York City's Department of Finance, which has a caseload of 120 such cases, adopted a policy in mid-2015 of notifying property owners whenever a new deed is recorded on the property, so they can challenge the transaction. Cook County (Illinois) officials have 62 open investigations of allegations of deed fraud. (*Id.* at 2.)

Shell Companies

A related form of fraud utilizes shell companies to get vulnerable homeowners to transfer the deeds on their homes, promising that they will have their debts paid and receive cash while continuing to remain in the homes. Once the deed is transferred, however, the fraudsters mortgage the property, leaving the original owner with the debt. Because one or more shell companies are involved, it is impossible to locate the "owner." (Stephanie Saul, *Real Estate Shell Companies Scheme to Defraud Owners Out of Their Homes*, NY Times, Nov. 8, 2015, *available at* www.NYTimes.com/2015/11/08/nyregion/Real-Estate-Shell-Companies-Scheme-To-Defraud-Owners-Out-Of-Their-Homes.html?_r=0.)

Shell companies organized as limited liability companies (LLCs) are able to operate without disclosing the identities of the true principals in the company. Deed thieves typically look for properties that are in poor repair, or have a mortgage in arrears, because the homeowners are likely to be willing to sign over the property in return for what they believe will be a solution to their financial problems. If the homeowner is unwilling, or the criminals do not want to approach them, a new deed can be created and the owner's signature forged. (*Id.* at 2.) To further obfuscate, the deed can be transferred to additional LLCs or corporations; it is a danger signal if the subsequent deed

recites a transfer for no consideration, or it is impossible to determine the identity of the transferee. (*Id.* at 3.)

Jacques Jiha, the commissioner of finance for New York City, has tried to fight deed fraud by requiring LLCs to disclose all their members to the city's tax auditors. However, this is not a complete solution, because some of the members are nominees, so the identity of the principals remains concealed. (*Id.* at 4.)

IDENTITY THEFT

Although identity theft is not limited to the elderly or disabled, these groups are especially vulnerable. Medical identity theft is the appropriation of identifying information, such as a Medicare number, which is then used to fraudulently obtain medical care or drugs. It also includes fraudulent billing for services or materials.

In October 2015, the U.S. Senate Special Committee on Aging held a hearing on the federal government's attempts to protect senior citizens from identity theft. Gary Cantrell, Deputy Inspector General for Investigations, HHS Office of Inspector General, testified that identity thieves can steal personally identifiable information and/or protected health information. (Gary Cantrell, testimony before the U.S. Senate Special Committee on Aging, *Protecting Seniors From Identity Theft: Is the Federal Government Doing Enough?* (Oct. 7, 2015), *available at* www.Aging.Senate.gov/imo/media/doc/OIG_Cantrell_10_7_15.pdf.) The theft can be committed by either health-care personnel or criminal enterprises, and can include using the identities of real patients to bill Medicare for nonexistent services. (*Id.* at 4.) Sometimes the patients are involved in the criminal activities—for instance, taking money to surrender their information, obtaining drugs, or getting kickbacks when the criminals defraud Medicare by billing for fictitious services. (*Id.* at 7.)

Maine Senior Medicare Patrol

Betty Balderston, the statewide coordinator for the Maine Senior Medicare Patrol (SMP, *www.MaineLSE.org/content/maine-smp*), explained that the SMP saved Medicare and Medicaid almost $1 million in 2014 in program savings and cost avoidance. (Betty Balderston, testimony before the U.S. Senate Special Committee on Aging, *Protecting Seniors From Identity Theft: Is the Federal Government Doing Enough?* (Oct. 7, 2015), *available at* www.Aging.Senate.gov/imo/media/doc/Balderston_10_7_15.pdf.)

The SMP warned about scam phone calls informing the recipients that new Medicare cards were being issued, and asking for their Medicare number, bank account information, and financial routing numbers. The SMP got the Maine Attorney General's Office to issue a consumer alert about this scam, asking victims to review their Medicare statements for at least a year, report to Medicare any suspicious items that appeared on the statements, and inform financial institutions about the possible compromise. (*Id.* at 2-3.)

Vulnerability of Social Security Numbers as Identifiers

Mark Rotenberg, president of the Electronic Privacy Information Center (EPIC, *www.EPIC.org*), testified that one of the greatest vulnerabilities in the data world is the use of Social Security numbers (SSNs) as multipurpose identifiers. (Mark Rotenberg, testimony before the U.S. Senate Special Committee on Aging, *Protecting Seniors From Identity Theft: Is the Federal Government Doing Enough?* (Oct. 7, 2015), *available at* www.Aging.Senate.gov/imo/media/doc/Rotenberg_10_7_15.pdf.) EPIC has asked Congress to prevent the use of SSNs as national identifiers since 1991; the GAO asked Congress to remove SSNs from government documents in 2004. (*Id.* at 4.) Data breaches are particularly common in health-care settings, and Rotenberg testified that using SSNs on Medicare cards increases the vulnerability of senior citizens to medical identity theft. (*Id.* at 6.)

Sean Cavanaugh, the HHS deputy administrator and director, testified that, as of April 2019, CMS will no longer use SSNs as the primary identifier on Medicare cards. At that point, Medicare beneficiaries will receive Medicare Beneficiary Identifiers, which will improve security because they can be canceled if the card is stolen or the number is otherwise compromised. (Sean Cavanaugh, testimony before the U.S. Senate Special Committee on Aging, *Protecting Seniors From Identity Theft: Is the Federal Government Doing Enough?* (Oct. 7, 2015), *available at* www.Aging.Senate.gov/imo/media/doc/CMS_Cavanaugh/_10_7_15.pdf at 1.) Cavanaugh warned that the transition process will be difficult and expensive ($230 million has been appropriated), because many IT systems in the federal and state governments and private industry will have to be updated. (*Id.* at 2.)

IRS Tips to Protect Identity

The IRS suggests the following seven steps for identity protection:

1. Review all credit card and bank statements frequently, and observe any suspicious charges. The IRS points out that banks, card issuers, and the IRS never email and ask for sensitive personal information, so any email that does so is part of a fraud scheme.
2. Review and respond to all IRS correspondence, because it can indicate that your identity has been stolen and used to file a fraudulent return. References to employers for whom you have not worked or income you did not receive also could indicate fraud.
3. Free credit reports from the three major reporting agencies may be acquired at *www.AnnualCreditReport.com*; the IRS suggests checking each report at least once a year.
4. Review Social Security statements (or view them at *www.SSA.gov*) to see if the income statement shows more income than you actually earned.

5. Check health insurance statements to see if they reflect care you did not receive or claims that you did not file. (It is common to tap into other people's health insurance to pay for care.)
6. Do not discard documents with personal information, especially Social Security numbers, in ordinary trash; the documents should be shredded instead.
7. The IRS recommends having tax refunds directly deposited to prevent diversion of checks. (IRS, *Seven Steps for Making Identity Protection Part of Your Routine*, IRS Security Awareness Tax Tip Number 3 (Dec. 7, 2015), *available at* www.IRS.gov/uac/Seven-Steps-for-Making-Identity-Protection-Part-of-Your-Routine.)

NCLC WEBINAR ON UNAUTHORIZED PAYMENTS

On November 24, 2015, Lauren Saunders and Lauren Mahoney, from the National Consumer Law Center (*www.NCLC.org*), presented a webinar on unauthorized bank payments. (*Protecting Your Bank Account From Unauthorized and Recurring Payments*, *available at* www.NCLC.org/images/pdf/conferences_and_webinars/webinar_trainings/presentations/2014-2015/ProtectingYourBankAccount.pdf.) It is part of a series of free webinars, which will be continued in 2016, dealing with restoring public benefits to victims of financial exploitation, recovering misappropriated assets, and related topics. The webinar explained the legal rights of a person whose credit, debit, or prepaid card has been debited with unauthorized charges, and how to remedy fraudulent recurring charges to an account.

PINs and other financial information can be obtained by watching a legitimate user at an ATM or via phishing emails. If chip cards are left too long in the machine, the information can also be obtained. Online sales may be accompanied by fine print—e.g., the terms and conditions the purchaser agrees to may include monthly charges to the purchaser's credit card.

Customer Liability

When a debit card is lost or stolen, federal law provides that the cardholder's maximum liability is $50, provided it is reported within two business days of the time the customer realizes that the card has been stolen or lost. Many credit card networks will waive the $50. If the report is delayed, the cardholder is liable for $50 in losses in the first two days, and up to $500 for usage of the card after the two days.

It is common for consumers, especially older consumers who find it difficult to go to the bank or to handle financial affairs, to arrange recurring debits for bills like utilities and rent or mortgage payments. Although this is convenient, it also renders them vulnerable to fraud.

If unauthorized charges appear on a bank statement, the customer has no liability if the charges are contested within 60 days of the statement. There is

also no liability for charges made in the first 60 days if the report is delayed, but the customer is liable for later charges that could have been prevented by making a prompt report.

Bank Obligations

The bank has an obligation to undertake an investigation, and either complete it within 10 days or make a temporary credit to the customer's account and complete the investigation in 45 days.

The customer is entitled to notification of the bank's findings. The bank has to show that the charge was authorized; it is not a defense for the bank if the charge was unauthorized and the bank blames the customer's negligence. If the bank concludes that the charge actually was authorized, it can debit the customer's account, but for a period of five business days, this debit cannot be used to "bounce" other items.

CFPB rules allow consumers to change their minds and revoke authorization for recurring charges; the CFPB website provides a sample letter for this purpose. Banks have an obligation to stop recurring payments if the customer gives written or oral notice three business days before the payment is scheduled. All future payments must be terminated. The bank can demand written confirmation and can require that the customer send a copy of the notice of revocation to the payee within 14 days. Banks are allowed to impose stop-payment fees.

Problems can be averted by using the bank's bill payment website instead of preauthorizing payments. Because of the way federal debtor/creditor law is written, it may be easier to revoke or contest preauthorized credit card payments than debits taken from a bank account. The customer should investigate the payee, authorize payments only to reputable companies that can be trusted, and keep track of the payments.

To make it more difficult for criminals to make unauthorized charges, customers can improve their password security and change passwords for different accounts. Writing the PIN on the debit card creates vulnerability.

CFPB Compliance Bulletin

A recent compliance bulletin from the CFPB reminds entities of their obligations under the Electronic Fund Transfer Act (EFTA). (CFPB, *Requirements for Consumer Authorizations for Preauthorized Electronic Fund Transfers*, Compliance Bulletin 2015-06 (Nov. 23, 2015), *available at* http://files.ConsumerFinance.gov/f/201511_CFPB_Compliance-Bulletin-2015-06-Requirements-For-Consumer-Authorizations-For-Preauthorized-Electronic-Fund-Transfers.pdf.) Preauthorized electronic fund transfers (defined as transfers authorized in advance to recur at regular intervals) require the customer's authorization, which must be signed or have an equivalent electronic signature. The customer must be given a copy of the authorization, explaining the key terms of the transaction, such as the timing and amount of the transfers.

(Zane A. Gilmer, *CFPB Releases Compliance Bulletin Related to Consumer Authorizations for Preauthorized Electronic Fund Transfers*, Stinson Leonard Street LLP, Nov. 29, 2015, *available at* http://Dodd-Frank.com/CFPB-Releases-Compliance-Bulletin-Related-To-Consumer-Authorizations-For-Preauthorized-Electronic-Fund-Transfers.)

FIGHTING EXPLOITATION OF FACILITY RESIDENTS

Preventing financial exploitation, including tips for ombudsmen and facilities, was discussed by a panel at the Consumer Voice's November 2015 annual conference. The program was presented by the CFPB's Naomi Karp; Iris C. Freeman, Minnesota Elder Justice Center; and Sherry Kulp, the long-term care ombudsman for Kentucky.

The panelists presented the manual they wrote to protect facility residents, and explained how ombudsmen can adapt it to their own state's rules and use it as an advocacy tool. For example, state definitions of "elder," "vulnerable person," and "financial exploitation" are not uniform, and reporting requirements vary from state to state. (*Protecting Residents From Financial Exploitation*, 2015 Consumer Voice Conference, Arlington, VA (Nov. 4-7, 2015), PowerPoint *available at* https://TheConsumerVoice.org/events/2015-Consumer-Voice-Conference-Materials.)

All facility residents are entitled to receive quality care—which includes being free from neglect, abuse, and misappropriation of their assets. Ombudsprograms are covered by Title VII of the Older Americans Act, which includes activities for preventing elder exploitation, abuse, and neglect.

A senior citizen might be exploited by a family member, a paid caregiver, a residential facility staff member, a financial adviser, a contractor, or an individual scammer. Nursing home and ALF residents are particularly vulnerable, because they are likely to be cognitively impaired. They may be victimized by a person designated to manage their money, or robbed or coerced by employees of the facility. They are at risk of eviction if the exploitation leaves them unable to pay facility fees. The aim of the manual is to help facility management reduce the risk of financial exploitation of residents.

There should be an immediate investigation whenever warning signs such as the following appear:

- A resident's possessions disappear from the living unit;
- A resident is put under pressure to sign a document or make a financial decision;
- The facility's bills are not paid;
- Someone appears suddenly and claims to be in charge of the resident's finances or health care, but does not document this authority;
- The facility's staff or volunteers receive many or lavish gifts; or
- The resident writes (or allegedly writes) many checks made out to "cash."

The investigation should be fully documented. It is likely that a report will have to be made to the relevant authorities.

FIDELITY MOVES TO PROTECT CLIENTS

Fidelity Investments' research revealed that the vast majority of financial advisers (75%) have at least one client with diminished capacity, and 20% have encountered abuse of their elderly clients. Fidelity Clearing & Custody is the Fidelity Investments division that holds securities and performs clearing transactions for broker-dealers, registered investment advisers, and record keepers for retirement plans. In late 2015, Fidelity Clearing & Custody, in collaboration with the technology firm EverSafe (*www.EverSafe.com*), launched a program to cope with aging-related financial issues. EverSafe's monitoring service scans financial accounts and credit reports each day to spot identity theft and other forms of suspicious activity.

Warning Signs

For example, advisers should be on the lookout for changes in client behavior and should examine whether clients appear to be struggling with concepts that they once understood. It is a warning sign if clients miss meetings, appear at the wrong time, or have difficulty reading standard reports or using familiar forms. (Fidelity Investments, *Fidelity Clearing and Custody Launches Program to Help Advisors Protect Aging Clients From Financial Abuse* (Dec. 2, 2015), *available at* www.Fidelity.com/about-fidelity/Institutional-Investment-Management/Clearing-And-Custody-Launches-Program-To-Help-Advisors-Protect at 1.)

Proactive Measures

Advisers can also protect elderly clients by discussing possible future loss of capacity before signs of dementia appear, and helping them create durable powers of attorney and other relevant documents while it is clear that they still have capacity. There should be frequent phone contact, followed up with written memos of what was discussed, so that the adviser has ongoing insight into the client's mental state.

The Investment Policy Statement should be reviewed and revised at least once a year; the discussion can reveal whether a client is faltering. The client's credit card charges should be reviewed to see whether any improper continuing payments are being deducted (e.g., services that were not rendered, automobile insurance for clients who have stopped driving and no longer have a car or a driver's license). (*Id.* at 2.)

Fidelity's tools for advisers include the white paper *Dealing With Diminished Capacity as Clients Age: Ways to Help Mitigate Your Firm's Risk in Serving an Aging Client Base.* (*Available at* https://fiws.Fidelity.com/app/literature/white-paper/9865541/Dealing-With-Diminished-Capacity-As-Clients-age.html#!; video version *available at* www.Brainshark.com/fidelityiws/vu?pi=zIczbqHrTzIWXsz0&nodesktopflash=1.)