Frauds, Scams and Slams: Don't Fall Prey to Identity Theft

Janice M. Park, PhD
Gerontology Specialist

Most people make transactions that expose them to identity fraud. Every time they write a check, make a purchase at a retail store, purchase by credit or debit card, make a telephone order, or make an Internet purchase, there is a risk of identity theft. During the 1990s, a new breed of con artist, the identity thief, began ruining credit ratings. These con artists thrive on information shared every time someone makes a transaction. Identity thieves use someone's personal, identifying information without their knowledge to commit fraud or theft. All thieves need to become an imposter is personal information such as name, address, telephone number, cell telephone number, bank account numbers, Medicare card number, driver's license number, Social Security number, credit card and debit numbers, date of birth, and mother's maiden name.

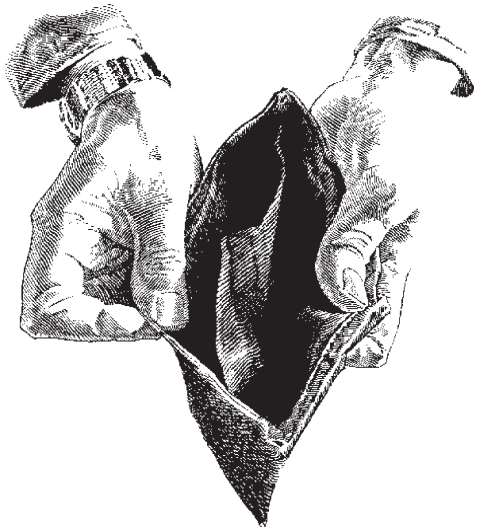
The Federal Bureau of Investigation considers identity theft as one of the fastest growing "white collar" crimes in the United States. In 2000, more than 500,000 consumers were victims of identity theft by an estimated 14,000 operators. Unfortunately, older adults fall victims because they trust others, have poor memory or cognitive impairment, and often are willing to share personal information over the phone or with someone at their door.

This crime has a devastating effect on victims financially, emotionally, and psychologically. Likewise, it has a detrimental impact on financial institutions. The five most common ways that identity thieves misuse information is to:

1. Open new credit card accounts
2. Change existing credit card accounts
3. Open new bank accounts
4. Obtain new loans
5. Obtain cellular telephone service

Legally, victims are not responsible for most of the money lost from unauthorized use of funds through fraud, but it can be difficult and time consuming to prove fraud occurred. Banking institutions must often withstand losses stemming from identity-theft-frauds of their customers. According to the Federal Trade Commission, victims pay an average of $1,000 in out-of-pocket expenses and spend hours correcting credit records.

Oklahoma Cooperative Extension Fact Sheets are also available on our website at:
http://osufacts.okstate.edu



How do identity thieves get personal information?

Identity thieves use a variety of low and hi-tech ways to obtain personal information. There is no way to completely guard all personal information, but being aware of ways that thieves get information can minimize the risk of someone gaining private information. The following are common ways con artists get personal information.

- Steal wallets and purses containing credit cards, checks, debit cards, Social Security cards, telephone calling cards, business cards, union cards, employer's identification cards, health insurance cards, or driver's license.
- Steal mail containing bank statements, credit card statements, investment statements, pre-approved credit card offers, insurance statements, credit reports, or end-of-year tax documents.
- "Dumpster diving" the trash including billing statements, discarded credit card offers, catalogs with address codes, mail order statements, credit card

slips, junk mail, loan applications, paycheck stubs, or medical records.
- Intercept information sent electronically such as e-mail, public pay phones, cellular phones, or cordless telephones.
- Obtain personal information shared over the Internet from unsecured sites.
- Obtain personal information from place of employment.
- Break into a home and steal current files, old tax records, and letters.
- Purchase personal data from "inside sources" such as employees at work, store employees, or financial institution employees.
- Obtain credit report or personal information by posing as someone with a legal right to information such loan officer, employer, or landlord.
- Complete a "change of address" form diverting mail to a different location.
- Obtain a bank account number and order new checks sent to a different address.
- Use "pretext calling" when contacting financial institution employees to pose as a customer to obtain personal account information, creating fraudulent accounts to sell to debt collection services, attorneys, or private investigators for use in court proceedings.

How do identity thieves use personal information?

Once thieves get the credit card number, they can call the credit-card company and request a "change of mailing address" for the account. The thief then makes charges on the card. Because the billing statement goes to the new address, it may be some time before something bad occurs. Therefore, it is very important that bank statements and credit card statements be checked for accuracy as soon as they arrive. Also, it is a good idea to keep a list of expected statements and the dates they arrive so the diversion can be discovered early.

When thieves obtain a Social Security number, date of birth, and mother's maiden name, they can open a new credit card account in your name and with their address. Unsolicited pre-approved credit card applications are easy for thieves to use to establish a new account. Accounts can be charged to the limit and individuals won't know the account exists until the unpaid account is turned over to a collection agency and the credit bureaus have placed the delinquency on your credit report. This can ruin credit. Many may not realize it until a loan application is turned down. It can take lots of time and aggravation to correct a credit history.

Identity thieves can also open bank accounts in another's name with their address and write bad checks on the accounts. They can also obtain loans using the stolen identity.

How can someone reduce the risk of being an identity theft victim?

One way to lower the risk of becoming an identity victim is to limit the amount of personal information carried. Be cautious about responding to e-mail or telephone requests for information supposedly needed to update account information, as this is likely a scam. Use only secure Internet sites when making purchases. Consider subscribing to an identity guard service, such as Privista (privista.com), or a credit bureau like Equifax. These services will monitor credit reports for 10 unusual activities, such as address changes, Social Security number changes, or new account openings. There is a charge for this service. Request an annual copy of a credit report from each of the three major credit bureaus in the U.S. (Equifax, Inc., Experian, and TransUnion) and analyze it for signs that someone has opened accounts or fraudulently misused existing accounts.

14 ways to protect personal information from identity thieves

- Do not carry a Social Security card. If a Social Security Number appears on other cards such as Medicare card, carry those cards separately.
- Do not carry passports or birth certificates, unless necessary when traveling.
- Never carry PIN numbers or passwords.
- Carry only a few.
- Do not carry deposit slips that have bank account numbers printed on them.
- Do not put a telephone number, a Social Security number, or driver's license number on checks.
- Do not put a Social Security number on a driver's license; get a different number.
- Do not store past years' tax documents in the garage.
- Cancel unused credit cards.
- Sign new credit cards as soon as they arrive.
- Do not give store clerks personal information when using a credit card, debit card, or check.
- Never share Social Security numbers, credit card numbers, a mother's maiden name, address, telephone numbers, or other personal information over the phone unless the call was initiated with a well known company.
- Shred all papers that contain personal information before discarding in the trash.
- Carry family member's telephone numbers, cellular numbers, addresses, or e-mail addresses separate from wallet.

Steps to take when a victim of identity theft

If someone has stolen an identity, there are many places and ways it can be used. As soon as you suspect someone has stolen personal information, take action immediately. The following are steps to take and agencies or institutions to notify. Don't stop by just calling credit card companies.

1. Immediately contact the fraud department of each of the three major credit bureaus and request a report from each credit bureau. A credit report costs approximately eight dollars, however it is free if it contains errors due to fraud, and if the request is made in writing.

Equifax, Inc. - www.equifax.com
To order a credit report, call 800-685-1111 or write:

PO Box 740241, Atlanta, GA 30374-0241

To report fraud, call 800-525-6285/ TDD: 800-255-0056 and write: Consumer Fraud Division, PO Box 740241, Atlanta, GA 30374-0241

Experian – www.experian.com
To order a credit report, call: 888-397-3742 or write: PO Box 2104, Allen, TX 75013-2104

To report fraud, call: 888-397-3742/ TDD: 800-972-0322 and write: Experian's National Consumer Assistance, PO Box 9532, Allen, TX 74013-9532

TransUnion - www.tuc.com
To order a credit report, call 800-916-8800 or write: Consumer Disclosure Center, PO Box 1000, Chester, PA 19022-1000

To report fraud, call: 800-680-7289/ TDD: 877-553-7803 and write: Fraud Victim Assistance Division, PO Box 6790, Fullerton, CA 92634-6790

- Request the bureaus place a "fraud alert" in the file to let creditors know you are a fraud victim and that no additional credit should be allowed without permission.
- Request that a "victim's statement" be filed asking them not to open any new accounts without contacting the individual first.
- Review reports immediately to make sure no additional fraudulent accounts were opened and no unauthorized changes were made to existing accounts.
- Look for the section of the report that lists "inquiries." If "inquiries" appear from companies that opened fraudulent accounts, request to remove them from the report.
- Allow a few months for changes to be made, then order new ones and make sure errors have been corrected and that no additional fraudulent activity appears.
- Learn about individual's rights under the Fair Credit Reporting Act.

2. File a complaint with the Federal Trade Commission (FTC). While the FTC does not bring criminal charges against an identity thief, they can help victims by giving them information to solve financial and other problems that result from identity fraud. The FTC will also provide complaint information to appropriate agencies or to private organizations that can take action. To file a complaint with the FTC call the Identity Theft hotline toll-free 877- IDTHEFT (438-4338): TDD: 202-326-2502 or by mail: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington DC 20580 or www.consumer.gov/idtheft. The FTC puts complaint information into a secure consumer fraud database and shares it with local, state, and federal law enforcement agencies.
3. Call credit and charge card companies, using their toll-free numbers and explain the problem. Request that the accounts be closed. Open new accounts with new numbers, PINs, and passwords and request password-only access. Get a new ATM card with a new PIN. Follow-up each telephone call with a letter detailing the situation. Keep copies and dates of all telephone calls and written correspondence. This will establish a "paper trail" and will be proof of required notification in a timely manner. Call all banks, other lenders, and telephone companies fraud or security representatives and explain the situation. Be sure to ask for the representative's name and send a detailed letter mentioning the telephone conversation and representative's name.
4. If a wallet is lost or stolen, immediately notify local police. The FDIC Division of Compliance and Consumer Affairs recommends that a police report be filed. Also, sign a written affidavit verifying that all unauthorized transactions in your name are fraudulent. These documents show that the individual had no part in any fraud and can be very important when dealing with a bank or credit card company to remove errors in credit report.
5. If bank checks are stolen or missing, contact the bank and stop payment. Contact major check verification companies and request that they notify businesses using their databases not to accept these checks.

National Check Fraud Service: 843-571-2134
SCAN: 800-262-7771
TeleCheck: 800-710-9898 or 927-0188
CrossCheck: 707-586-0551
Equifax Check Systems: 800-437-5120
International Check Services: 800-526-5380

Open new bank account(s) and get new checks beginning with a different block of numbers to cut down on confusion with old checks. Shred all old checks on hand.

6. If investment or brokerage accounts have been tampered, immediately contact broker or account manager, and report the fraud to the Securities and Exchange Commission.
7. If thieves have stolen mail that included bank and credit card statements, tax documents, or pre-approved credit card applications or other documents and have created new accounts or otherwise used the information to commit fraud, contact your local post office or the nearest postal inspection service.
8. If an identity thief has used personal information to set up new phone service accounts, including a cellular phone, or if they are using your calling card or PIN, call the service provider to cancel the account.
9. If someone has filed for bankruptcy using personal information, contact the U.S. Trustee in the region where the bankruptcy was filed. To find the telephone number, check the blue pages of the telephone directory or look under U.S. Government-Bankruptcy Administration.
10. Identity thieves can make a criminal record with an individual's name. When arrested they provide that personal information. In this situation, contact a lawyer.

The Identity Theft and Assumption Deterrence Act of 1998 makes it a federal crime when someone: "knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of federal law, or that constitutes a felony under any applicable state or local law."

The act specifies that a Social Security Number is considered a "means of identification." The act also states that a credit card number, cellular telephone, electronic serial number or any other piece of information that may be used alone or in conjunction with other information to identify a specific individual is considered a means of identification.

If specific companies or institutions do not respond to questions and complaints, contact the government agency with jurisdiction over those companies. Violations of this act are investigated by federal law enforcement agencies including the U.S. Secret Service, FBI, Postal Inspection Service, Medicare Fraud Unit, and Social Security Administration Office of the Inspector General. Federal identity theft cases are prosecuted by the U.S. Department of Justice. Identity fraud schemes generally involve violations of other statues as well, such as credit card fraud, computer fraud, mail fraud, wire fraud, financial institution fraud, Medicare fraud, Social Security fraud, or others. Many states also, have laws related to identify theft: Oklahoma has such a state law. Check the Oklahoma reference site at www.consumer.gov/idtheft

References

Consumer Action. (n.d.). Protect yourself from identity theft. Retrieved on January 24, 2002, from www.consumer-action.org.library/english/privacy/pv-f-03_en/pv-f-03_EN.html

Federal Deposit Insurance Commission. (Fall 1997). Your wallet: A loser's manual, FDIC Consumer News. Retrieved on February 2, 2005, from www.fdic.gov/consumers/consumer/news/cnfall97/wallet.html

Federal Trade Commission. (August 1997). Avoid credit and charge card fraud. Retrieved on February 5, 2002, from www.ftc.gov/bcp/conline/pubs/credit/cards.htm

Federal Trade Commission. (February 2000). Identity thieves can ruin your good name. Retrieved on February 5, 2002, from www.ftc.gov/bcp/conline/pubs/credit/identity/index.html

Federal Trade Commission. (February 2000). FTC Consumer Alert: Identity crisis: What to do if your identity is stolen. Retrieved on February 5, 2002, from www.ftc.gov/bcp/conline/pubs/alerts/idenalrt.htm

Federal Trade Commission. (February 2001). When bad things happen to your good name. Retrieved on February 5, 2002, from www.ftc.gov/bcp/conline/pubs/credit/idtheft.htm

Know Fraud: Focusing on ID Theft. (Revised 07-30-2001). Retrieved on April 26, 2001 from www.consumer.gov/knowfraud/index.html

Office of the Comptroller of the Currency (OCC). (n.d.). Identity theft and pretext calling. Retrieved on February 5. 2002, from www.occ.treas.gov/idtheft.pdf

Social Security Administration. (July 2001). Social Security: When someone misuses your number. (SSA Pub. No. 05-10064), Retrieved on February 5, 2002, from www.ssa.gov/pubs/10064.html

Issued in furtherance of Cooperative Extension work, acts of May 8 and June 30, 1914, in cooperation with the U.S. Department of Agriculture, Robert E. Whitson, Director of Cooperative Extension Service, Oklahoma State University, Stillwater, Oklahoma. This publication is printed and issued by Oklahoma State University as authorized by the Vice President, Dean, and Director of the Division of Agricultural Sciences and Natural Resources and has been prepared and distributed at a cost of 20 cents per copy. 0407 GH.