consumer action

Education and advocacy since 1971

Theft of a Deceased Person's Identity

The dead have always been vulnerable to identity theft, but years ago fraud criminals would have to study death notices and obituaries or hang around funeral homes to obtain a decease person's personal information. Today, with so much of our personal data being entered into electronic databases, stored on electronic devices or floating around in the 'ether' of the Internet, everyone—including the deceased—is vulnerable to having their identity cloned or stolen (or "ghosted," as AARP calls it).

What is ghosting? According to AARP, ghosting occurs when a deceased individual's personally identifiable information is stolen to commit fraudulent acts such as account takeover, taxpayer ID theft and tax refund fraud, medical ID theft, driver's license ID theft, or to apply for new credit cards and loans, and even to secure employment, utility services or telecommunications services.

What can be done? According to the Identity Theft Resource Center (ITRC), although the Social Security Administration (SSA) maintains a Death Master File, and all three major credit reporting agencies (CRAs) and most financial institutions subscribe to monthly updates, it can take up to 60 days for a name to make it onto the list. In most cases, a funeral director will report the person's death to the SSA (Statement of Death by Funeral Director). However, delays in the SSA's transmission of the Death Master File to the financial industry can provide time for ID thieves to collect enough personal information to open credit accounts or take other fraudulent actions using the deceased's information. Until the credit reporting agencies and creditors are notified of the death, the accounts of the deceased will remain open. The ITRC reports that an active credit account can remain open for up to 10 years without activity.

The following steps are recommended by the ITRC for all deaths, regardless of age:

1) Obtain at least 12 copies of the official death certificate when it becomes available. In some cases you will be able to use a photocopy, but some businesses will request an original death certificate. Since many death records are public, a business may require more than just a death certificate as proof.

2) If there is a surviving spouse or other joint accountholder, that individual should immediately notify relevant credit card companies, banks, stockbrokers, loan/lien holders and mortgage companies of the death.

3) The executor or surviving spouse will need to identify all outstanding debts and determine how they will be dealt with. You will need to transfer the account to another person or close the account. If you close the account, ask the creditor to list it as: "Closed. Account holder is deceased."

4) Contact all credit reporting agencies, credit issuers, collection agencies and any other financial institutions that need to know of the death, following the required procedure for each one. (Each CRA has different reporting procedures on its website). You can use a sample letter in the MoneyWi$e ID Theft lesson plan (www.consumer-action.org/modules/articles/id_theft_account_fraud_lesson_plan) to notify each CRA that your loved one is deceased. It may be a good idea to send everything by certified mail, returned receipt requested.

5) Order a copy of the decedent's credit reports. (Note that you must contact each agency for specific instructions.) If you suspect that someone is fraudulently using the information of a deceased person, and you are the surviving spouse or executor of the estate, the ITRC recommends that you place a "Deceased alert" on the report. Notify the police department in the decedent's jurisdiction. If you have evidence of fraud, such as

collection calls, notices or bills coming in the mail, or if you find open fraudulent accounts on the credit report, notify the credit issuers, collection agencies and utilities or telecommunications companies that your loved one is deceased and couldn't have opened the accounts. Provide each with a copy of the death certificate and other supporting documents as proof. Remember, ID theft can be an inside job, so in the event that the thief is a family member, it may be best to seek professional advice on a course of action from a family law attorney.

6) Review each credit report, looking for active credit accounts that still need to be closed or any open collection accounts that should be dealt with. Be sure to ask for all contact information on accounts currently open in the name of the deceased (credit granters, collection agencies, etc.) so that you can follow through with those entities. Request that the report be flagged with the following alert: "Deceased. Do not issue credit. If an application is made for credit, notify the following person(s) immediately: [List the next surviving relative, executor/trustee of the estate and/or local law enforcement agency, noting the relationship]."

Other groups to notify:

- Social Security Administration
- Insurance companies (auto, health, life, etc.)
- Veteran's Administration (if the person was a former member of the military)
- Immigration Services (if the decedent is not a U.S. citizen)
- Department of Motor Vehicles (if the person had a driver's license or state ID card; make sure that any vehicle registration is transferred to the new owner)
- Professional licensing agencies (Bar association, medical board, cosmetology board, etc.)
- Any membership programs (video rental, public library, fitness club, etc.)

Resources:

Identity Theft and the Deceased: Prevention and Victim Tips (ITRC): www.idtheftcenter.org/Fact-Sheets/fs-117.html

How to Prevent Identity Thieves from Impersonating a Dead Relative (Credit Sesame): www.creditsesame.com/blog/identity-theft-of-dead-relative/

Protecting the Dead From Identity Theft (AARP): member.aarp.org/money/scams-fraud/info-03-2013/protecting-the-dead-from-identity-theft.html

Identity Theft: What to Do If It Happens to You (Privacy Rights Clearinghouse): www.privacyrights.org/content/identity-theft-what-do-if-it-happens-you

Digital Estate Planning Guide (Consumer Action): www.consumer-action.org/downloads/english/Digital_Estate_Planning_Guide.pdf

Identity Theft After Death: How to Keep Crooks from 'Ghosting' Deceased Loved Ones (TheStreet): www.thestreet.com/story/13170823/1/identity-theft-after-death-how-to-keep-crooks-from-ghosting-deceased-loved-ones.html

Consumer Action empowers low- and moderate-income and limited-English-speaking consumers nationwide to financially prosper through education and advocacy. Visit us online at www.consumer-action.org.