EVEN AFTER DEATH, IDENTITY THEFT IS A RISK

It's been estimated that nearly 15 million people annually have their identities stolen in the United States. And, nearly 2.5 million of them are dead, according to ID Analytics.

Identity thieves target people who have passed away, in addition to stumbling upon the dead by illicitly obtaining Social Security numbers. The crime often goes months or even years before being noticed.

Thieves grab personal information from funeral homes, hospitals, nursing homes and published information. It could be as easy as skimming the obituaries for critical information and illegally purchasing matching Social Security numbers on the Internet.

In other instances, identity thieves are able to obtain this information from a patient's records while they are admitted to a healthcare facility.

SAFEGUARDING AGAINST THEFT

There are numerous measures that should be taken to protect against identity theft for those who have recently passed.

Obituaries shouldn't list the birthday, mother's maiden name or other personal identifiable information that could be used to obtain credit cards, loans, etc.

Don't include the address of the deceased because burglars comb listings to learn when families will be at a funeral or away from home.

A "death alert" should be communicated to the major credit bureaus – Trans Union, Equifax & Experian – who will alert anyone running credit reports or granting credit to that individual. You may have to provide a copy of the death certificate to them.

Banks, brokerage houses, insurers and credit card companies should be notified as soon as possible. Potential death benefits may be available to survivors or heirs of the individual, and the issuer is put on notice not to accept future charges or grant additional credit.

As accounts are closed, note that the owner is deceased to prevent future solicitation calls, etc. When communicating to these organizations, consider sending correspondence by certified receipt mail to maintain a documented trail of communication.

Survivors should promptly shut down social media profiles of the deceased, along with their email accounts. Since most passwords can be easily compromised, keeping the accounts active allows the risk to continue.

Insist that nursing homes, hospitals, etc., "mask" or truncate the Social Security number and full date of birth from all visible patient records unless completely necessary. Inquire about safeguards or security protocol used to protect this information.

The Department of Motor Vehicles should also be informed. The deceased's driver's license should be canceled to prevent duplicates from being issued to identity thieves.

Likewise, cancel the passport if the deceased had one.

Credit cards, driver's license, passport, etc. should be destroyed. The name should be removed from joint accounts.

Once financial affairs have been settled, old bank and credit card statements should also be shredded. Destroy old prescriptions or prescription bottles that contain personal health information.

The hard drive of the computer the deceased used should be rendered useless to prevent the recovery of vital information.

In addition to monitoring the mail for a deceased individual, suspicious activity can also be monitored by running a credit report on them at periodic intervals afterword. Free reports are available online.

A death should be reported as soon as possible to the Social Security Administration. Not only is a small death benefit available, but in some cases, enhanced survivor benefits may be obtainable. Once reported, benefits to the deceased will promptly cease.

WHO IS RESPONSIBLE?

In most cases, surviving family members are not personally responsible for the damage caused by identity thieves. But it's imperative to remove their names from joint accounts to prevent an issuer from attaching liability to a surviving spouse.

The estate may have a more difficult time. Defrauded banks, credit cards and cell phone companies may seek to recover their losses from the estate.

The same protections and defenses are available, similar to an individual, but the administrator of the estate will have to prove when and what occurred.

If you've ever been personally involved in something similar, you realize that this process is frustrating, timely and costly.

Now, more than ever, careful consideration should be given to selecting someone who can devote the proper attention to winding down the affairs of someone who has died.

Should you have questions regarding identity theft or need help filing Form 14039 (Identity Theft Affidavit) with the IRS, please give us a call at 251.473.5550 or send an email to info@rtbh.com. For other identity theft resources, we recommend visiting the following website www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft.