

AMERICA'S LEADING IDENTITY RESOLUTION AND EDUCATION SERVICE

## THIS MONTH'S TOPIC...

# Exploiting the Dead

### Never a victimless crime

As if families grieving the loss of a loved one don't have enough on their minds already, there comes an especially distasteful form of identity-related fraud: scamming the deceased. And it can create heartache and financial devastation for those least in need of additional trauma.

This month's article, [The Business of Exploiting the Dead](#) looks at the different ways the crime might present itself, the vulnerabilities that can allow it to transpire, and tips you can take to help protect yourself and your family. The [accompanying piece on Louis Taylor](#), meanwhile, investigates the personal toll identity thieves had on one family in the wake of a loved one's passing. In this month's editorial, [The New Level of Guardianship](#), we weigh in on the problem from the perspective of personal accountability when it comes to safeguarding our loved ones' personal data. We are the ultimate guardians of our own identities, but we must advocate for our loved ones in their time of need, too.



For a complete newsletter archive, visit: [www.identitytheft911.org/newsletters](http://www.identitytheft911.org/newsletters)  
To learn about the latest scams on identity theft, visit: [www.identitytheft911.org](http://www.identitytheft911.org)  
Comments, questions? Contact us: [newsletter@identitytheft911.com](mailto:newsletter@identitytheft911.com)



# The Business of **EXPLOITING THE DEAD**

Of all the identity theft cases he has worked, Larry Wilson says the ones involving the deceased are the toughest. Surviving wives, husbands and children are already grieving their loss. When they discover that their deceased loved one's identity has been stolen by a con artist, some find the pain and anger too much to bear.

"These people just lost their husband or wife," says Wilson, founder and director of the Identity Theft Victims Support Group of North America. "They're already having a terrible time, and then they start getting all these calls from collection agencies, which can get very, very nasty. It's sad to see." ▶

## An old crime...

Stealing a deceased person's identity is perhaps one of the oldest forms of identity theft. Classic stories of one person stealing the identity of another often involve the great themes of literature: a pauper posing as a prince to win the hand of a princess, or a son of nobility escaping the duty of war. But in the 20th century, identities came to have financial value as well. The creation of a national income tax in 1913 meant that the U.S. government needed to track the identities of its citizens to assure that they were working the jobs they claimed, so they could be levied the appropriate taxes. Assuming the identity of an unemployed person, or a dead one, became a simple way to avoid paying taxes.

The creation of social welfare programs in the 1930s, including Social Security, and the later addition of Medicaid and Medicare, added new systems of identity tracking by the government, and new incentives to steal the identities of others – either for tax evasion, or to steal the benefits of someone else.

With each evolutionary step away from gold and paper currency, financial institutions also bestowed monetary value on individual identities. Early on, check kiting became a lucrative way to buy goods fraudulently by presenting oneself as someone else. The value of stolen identities multiplied in the 1950s when Diners Club and American Express created the first credit cards, which in many cases did not even require a falsified government ID to make bogus purchases.

### ... With many variations

Different people value the identities of the dead for different reasons, however. One reason is that a living person hopes to shed his old identity completely and live his life under the name of the deceased. This is the most intimate type of identity theft, and it has its own name: "Ghosting." Many people who engage in ghosting are convicted criminals who hope to escape their rap sheets and begin a new life.

One recent example is former Serbian leader Radovan Karadzic, who took the name of Dragan Dabic, a Serb killed in Sarajevo in 1993 by military snipers directed by Karadzic. To escape prosecution for war crimes, Karadzic stole the dead man's name from a database of missing Serbs, and used it to take up a new life as an alternative medicine healer. Karadzic was arrested in July 2008.

"In ghosting, you want to become that person," says Kevin Paget, a Law and Science Fellow with the National Clearinghouse for Science, Technology & the Law at the Stetson University College of Law. Paget researched ghosting and other forms of identity theft involving the deceased. "The biggest advantage of a dead person versus a live person is the dead person is going to offer up a lot less resistance."

### Federal laws offer some protections, some concerns

Federal laws do provide a modicum of protection from identity theft to survivors of the deceased. They also create little-known vulnerabilities. Under the Health

Insurance Portability and Accountability Act of 1996 (HIPAA), a deceased person's medical records may only be released to a) the personal representative assigned by a court or named in a will to settle the person's affairs, b) a funeral director or medical examiner, or c) a relative, if the information could possibly impact that relative's health. Violations are punishable by up to \$50,000 in fines and a year in jail.

But it's that last provision, about relatives, that could provide an opportunity for crafty identity thieves to take advantage of family members' deaths. Say for example that the deceased person suffered from diabetes, a disease that is often hereditary. Under HIPAA, a family member could call the hospital and legally obtain the dead person's medical records simply by saying that they have

**"In ghosting, you want to become that person. The biggest advantage of a dead person versus a live person is the dead person is going to offer up a lot less resistance."**

**Kevin Paget, a Law and Science Fellow with the National Clearinghouse for Science, Technology & the Law at the Stetson University College of Law**

diabetes or pre-diabetic symptoms (which together affect 80.6 million Americans, according to the American Diabetes Association). The family member could then use the deceased's Social Security number, credit account numbers and medical ID number to obtain medical treatment without facing any penalties under HIPAA (though identity theft laws would still apply).

Identity theft is often perpetrated by someone close to the victim. Without realizing it, Congress may have created an obscure new avenue for identity thieves to obtain Social Security numbers



and other important identity data that didn't exist before HIPAA was created.

Another major federal privacy law, the Health Information Technology for Economic and Clinical Health (HITECH) Act, also offers protection with caveats. Signed into law by President Obama in February, HITECH requires institutions to notify next of kin if a deceased person's identity information is stolen or lost in a data breach. But institutions only need to send out notification notices if they know that the individual is deceased, and if they already have the address of the next of kin or personal representative, according to an analysis by Barnes & Thornburg, a large corporate law firm

**“It's pretty common that they go into a Wal-Mart or some big box store, buy a TV or some piece of electronics, and sell it on the black market for cash. That's the simplest way to do it.”**

**Larry Wilson, founder and director of the Identity Theft Victims Support Group of North America**

headquartered in Atlanta. An institution is not required to figure out whether anyone mentioned in its lost data is deceased, nor is it required to obtain contact information for the next of kin if it did not already have that information when the breach occurred. This means that relatives of the deceased may be held responsible for credit charges they know nothing about, and can't even take steps to clear their names or rebuild their own credit ratings until they start receiving notices from collections agencies.

This is the perfect example of why it's important to carefully organize your financial documents and to have a will, no matter your age. If your bank loses your personal information to a hacker

after you die, your family may never find out until the stolen information is being used to raid their bank accounts. But if they have a schedule of what credit accounts you opened and when you opened them, they may be more sensitive to news alerts about data breaches at your credit card company and use that information to find out whether they're at risk. Providing family members with a clear roadmap to your finances is an easy way to help them protect themselves.

### **Simple fraud**

Other cases of stealing the identities are even more straightforward. Michael Puopolo suffered a heart attack on March 25, 2008 while he was sitting in his car. He was transported to emergency room at Sentara Bayside Hospital in Virginia Beach, where he was pronounced dead.

Six hours later, a nurse from the emergency room, Matthew Wiseman, appeared at a Best Buy store. Wiseman, still dressed in his hospital scrubs, used Puopolo's Visa card to buy a laptop for \$1,800, prosecutors told the *Virginian-Pilot* newspaper. Wiseman pleaded guilty to credit card theft and credit card fraud. He was sentenced to a month in jail and eight years of probation.

“It's pretty common that they go into a Wal-Mart or some big box store, buy a TV or some piece of electronics, and sell it on the black market for cash,” Wilson says. “That's the simplest way to do it.”

These simple cases are often crimes of opportunity. For years, Ralph Lee Guttormsen lived with his roommate, Robert Sterling, in Monterey, California. When Sterling died of medical problems in the home in 2002, Guttormsen assumed his roommate's identity.

Using his friend's driver's license, Guttormsen opened credit cards, withdrew money from Sterling's bank account, and cashed checks using Sterling's identity “all over the Monterey Peninsula,” Thomas Uretsky, police commander for the city of Pacific Grove, told the *San Francisco Chronicle* in March, 2006.

The scam lasted for four years. Guttormsen was able to get away with it because he didn't open any new accounts in Sterling's name. Doing so would have raised alarm bells with financial institutions, which check the Social Security Administration's “Death Index” to make sure that a person is still alive before issuing him a new credit account. But by using an existing account, Guttormsen flew under the radar until he was pulled over by police for a traffic violation and offered Sterling's driver's license as his own.

“In many cases, ghosting doesn't look much different than other forms of identity theft,” Paget says.

### **Not-so-simple fraud**

Other scams are more sophisticated. Some thieves find the records of multiple dead people, either by reading newspaper obituaries or consulting the Social Security



Administration's Death Index. They combine the names of the dead with Social Security numbers and other identity information from other people, living or dead, to create new, synthetic identities that are difficult to track.

"Most of the cases we see involving dead people are synthetic identity theft," says Gina King, Manager of Fraud Operations for Identity Theft 911.

Armed with stolen credit card numbers and other information, thieves can use online stores to test whether the credit card numbers they're using have sufficient credit in their accounts to make purchases.

Testing is also important because of new federal Red Flag rules, which require companies to stop and check a credit application if it raises warning signs of identity theft. "Especially now, the test buy is important because stores and creditors have to pay attention to red flags," says Eduard Goodman, Chief Privacy Officer of Identity Theft 911. "If a person is deceased, that's a big red flag."

If the thief finds an apt victim, it touches off a buying spree to obtain merchandise that can be sold on the black market. These purchases are made as soon as possible after the victim's death, before family members have a chance to report the death to creditors. This reduces the chances of getting caught. "Right when someone passes away is the most opportune time for criminals," King says.

## Nothing simple about it

People don't always steal the identities of the deceased for strictly financial reasons, however. Some are just plain bizarre. The original version of *The Paper Trip*, a book published in the 1970s by a leftist publishing company called Eden Press, gave step-by-step instructions for underground activists on how to steal a dead person's identity. Now in its third edition, the book urges people to resist Big Brother's "Nazi-minded effort to control records" by creating "exactly the kind of Alternate Identity you need."

The purpose of this new identity is to help criminals escape prosecution. The Eden Press Web site covers this motive with the thinnest of fig leaves, saying that such a new identity will "eliminate problems from negative records" and allow people to "become 'invisible' to investigators who want to sue you."

## Whatever the crime, similar results

Few forms of identity theft are as old, or as varied, as stealing the identities of the dead. It also provides cover for crimes either traditional or bizarre, from standard credit card fraud to pedophilia.

In most cases, the impact on the families is the same: Huge legal bills spent trying to clear their credit histories of fraudulent charges, and thousands of hours wasted trying to salvage their loved one's good name.

"I've seen relatives of the deceased spend thousands of dollars and the next three years of their lives fighting to recover from identity theft," Larry Wilson says. "People attack them at their weakest point, which is absolutely sick." ■

## End-of-Life Planning Tips

*End-of-Life planning doesn't begin and end with purchasing life insurance.*

*To ensure that your family isn't victimized by identity theft after your – or a loved one's – death, experts recommend that everyone take the following the precautions:*



Use your power. As executor of your loved one's estate, you can notify the three major credit bureaus that the person is deceased, get copies of their credit files, and ask that the credit reports be shut down. All it requires is proof that you are the executor, and a certified copy of the death notice. This will prevent anyone from using the decedent's name to obtain credit. Quickly familiarize yourself with a schedule of the deceased's accounts so you can protect the estate.

Consider placing a freeze on your credit file, especially if you don't plan to make credit card purchases anytime soon. This is easier in states like Texas, which have "quick thaw" provisions in their credit freeze laws that allow consumers to call ahead and unfreeze their credit before they make major purchases.

Secure your documents. Make sure your identity documents are secure. Keep your birth certificate and passport in a bank safe deposit box. Keep all of your important records in a locked file cabinet, and make sure that your spouse or someone else you trust has a spare key. These basic precautions will help protect you while you're living, and protect your family's financial well-being after you've passed away.

# CASE STUDY: LOUIS TAYLOR

Louis Taylor died of natural causes in 2002. He was 78.

In 2009, he applied for a job. That's what a woman claimed, anyway, when she called Taylor's widow asking for more information about him. An hour later, another person called with questions about Louis's college application.

Taylor's widow explained that Louis was deceased. "Someone has played a dirty trick on him," the would-be employer said.

Despite that Louis Taylor had passed away seven years ago, within two days, his widow received phone calls from eight different people trying to pry information from her about her deceased husband.

"I was really angry," says Dan Taylor, 59, Louis's son. "I wanted to find out who these people are."

Someone was trying to "ghost" Louis Taylor. Ghosting involves stealing the identity of a deceased person, often for financial gain. In this case, the identity thief already had Louis Taylor's name, home address and phone number. All he or she needed was one more piece of information – a Social Security number, or perhaps a credit card number – to apply for credit in Taylor's name and start making fraudulent purchases.

That's why the scammers posed as employers or university officials, Dan Taylor believes. With the widow on the phone, the thieves could pretend to be innocent bystanders, claiming that some unknown third party had applied for a job using the deceased person's information. The widow simply needed to provide the correct information so the employer could verify their records.

Even more suspicious: Calls from multiple schools and employers all came from the same Missouri telephone number.

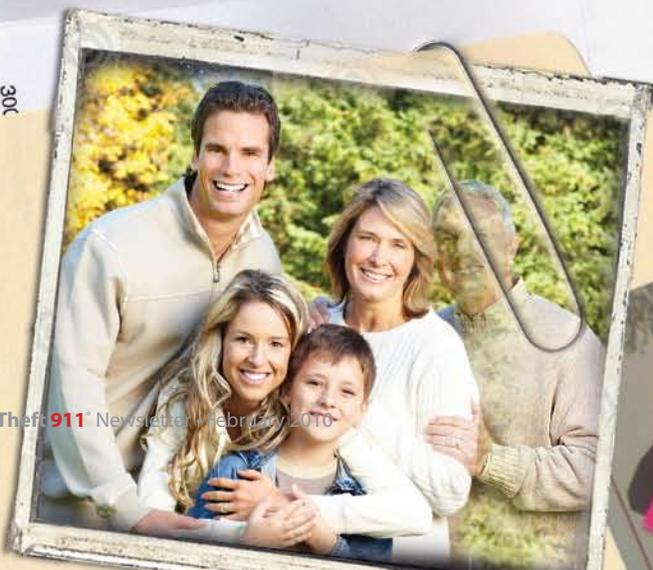
"My mom was quite upset that someone was calling for my dad saying he had applied for a job," Taylor says.

Confronting the elusive thieves proved difficult, however. When Taylor took the phone from his mother to demand answers, the callers hung up. Taylor tracked many of the calls to a phone in Missouri, but could not determine which phone company serviced the line.

Meanwhile, Taylor's concerns only grew. If the thieves managed to obtain that one additional piece of data, it could ruin his mother's credit rating and her ability to use her credit cards. To protect her, Taylor called all three credit bureaus and informed them of his father's death. He asked them to lock down his father's Social Security number and close all the credit accounts in his father's name. He also placed a freeze on his mother's credit cards that only she can lift if she ever needs to make a purchase.

Now Dan Taylor, his mother's finances, and his father's name are all protected from ghosting identity thieves. But that hasn't stopped the thieves from trying. Once or twice a week, Louis Taylor's widow still receives calls asking about her husband.

"My mother is savvy enough to hang up on them," says Taylor. "It's very surprising to me that this is happening seven years after my father passed away." ■





**W**hen criminals steal identities of the dead, surviving family members are the true victims. An already morbid crime becomes an out-and-out heinous one. While grieving their loss, survivors must then endure the painful ordeal of rebuilding the decedent's financial reputation and good credit standing, or face the prospect of either paying fraudulently incurred debts themselves or witnessing an estate wither away.

Sure, there are laws and procedures in place to help stop criminals from obtaining credit in a deceased person's name. The Red Flags Rule — a provision of the 2003 Fair and Accurate Credit Transactions Act — requires that banks (and, if and when Red Flags are fully enforced, will extend to car dealers, medical providers, and any other company, government agency or nonprofit group that extends credit) verify, among other things, credit applications for indications of identity theft. If they detect any warning signs, these entities must have a process in place for how to respond. This could include not extending credit to the individual in question, or notifying the police.

It's a partial solution, but not all credit-issuers are required to

## **Welcome to Accountability 2010. Regardless of the volume of laws enacted or the vigor with which those laws are enforced, the ultimate guardian of the consumer is the consumer. If we don't get that concept, criminals have that much more leverage over us.**

adhere to Red Flags, at least not for the time being. And even if — and when — they are required to do so, consumers can not happily and contentedly assume that all credit issuers will actually follow the law.

Then there's the Social Security Death Index — a useful tool for creditors looking to verify that their credit applicant is not, in fact, dead. That is, as long as they're checking the index months down the road. The problem with the Social Security Death Index is that there can be a lag time of days, weeks or months — the equivalent of a dog year for identity thieves — before a person's death is recorded. In the meantime, there exists a fertile landscape for financial devastation, and there are

folks out there who thrive on exploiting such a perfect criminal opportunity.

So what then? Where does that leave consumers? Well..... no doubt, some lawmakers are working to the best of their ability to help protect consumers from fraud, and businesses, if they know what's good for them (and their bottom line) should follow those laws and procedures. However, consumers can not — and should not — assume that government and business alone will keep their loved ones' names out of the criminal mire.

Welcome to Accountability 2010. Regardless of the volume of laws enacted or the vigor with which those laws are enforced, the ultimate guardian of the consumer is the consumer. If we don't get that concept, criminals have that much more leverage over us.

### **What's being ignored**

There's a giant issue that people aren't giving enough airplay, and it's that these measures address preventing theft with information that has already been stolen. But what about

actually working to protect sensitive personal information in order to prevent its theft in the first place?

First, let's look at where the standard

risks lurk. With ghosting, the thief could be a home health care worker, a hospital employee, a random stranger who cases obituaries like cat burglars case houses, or — most disturbing of all — a family member or so-called friend.

Elderly and infirmed family and friends need us to be their frontrunners. Make no mistake, if we find ourselves too overwhelmed in the caretaking process to want to deal with shoring up their finances and identity information, there's someone out there who is eagerly waiting to capitalize on our distraction.

For some reason, too many of us assume that keeping



watch over one's identity and finances is a remarkably time-consuming and effort-intensive process. It isn't. However, undoing the handiwork of an identity thief is. So start with your home base: Lock up your loved one's sensitive documents in a safe. Keep an inventory of all sensitive information, and check on it regularly. If you're in charge of their accounts, screen them with a hawk's diligence. If you're not in charge of their financial affairs, start — and maintain — a dialogue with them about keeping their data and accounts safe. If you have to be the warden over their living space — be it at home or a health care facility — do it. Know who visits them. Know who is caring for them (if you aren't). And don't permit their credit or bank cards or sensitive documents to remain at the health care facility or lay out in the open at home.

When the unfortunate — and inevitable — occurs, be aware of the very ugly reality that there are indeed strangers who comb obituaries in hopes of harvesting information for committing fraud. Don't give them an easy lay-up. It's understandable to want to pay tribute to your loved one, just be judicious with the information you publish in the newspaper or on your Facebook wall.

Next, suppress their credit file. This is probably the single-most important thing that can be done to protect their accounts from criminal manipulation. Contact each of the three major credit bureaus — Equifax, TransUnion and Experian — and make sure you're able to prove you are the executor and have a certified copy of the death notice on hand. Compared to the logistical nightmare and emotional dislocation involved when a loved one's information is being misused, these are minimal requirements. Credit bureaus may not be able to accommodate a request to suppress credit in every instance, but they are often willing to add certain types of protection on a deceased

person's credit file. It may be an alert — a red flag signaling creditors that they need to take additional steps toward authorization — or it may be a freeze, which basically prevents creditors from pulling a person's credit file, thus preventing the opening of new accounts.

### **Clearly still work to be done**

If health care workers are still preying upon the elderly and infirmed, that means government and business are still leaving the door open to fraud and exploitation. If health care providers can't be bothered to conduct and abide by thorough criminal background checks, then the government needs to require them to do so. And if providers fail to do so, they must be held to exacting penalties.

## **When the unfortunate — and inevitable — occurs, be aware of the very ugly reality that there are indeed strangers who comb obituaries in hopes of harvesting information for committing fraud. Don't give them an easy lay-up.**

This is a humble request. Husbands, wives, siblings, children, or dear friends must cultivate a safe and protective refuge for loved ones in their time of need. We must work to protect their good name and their memory. Tending to their identity and finances comes with this territory. Business owners and lawmakers: take a good, hard look at what's happening out in the world and how criminals continue to exploit the elderly and the ill, and start working now to ensure that we keep up with the ugly deeds of those who clearly have no conscience. This is the very least we can all do. ■

