

Good Housekeeping

[Click to Print](#)[Close](#)

The ID Theft You Haven't Heard of...Yet

They're not just going on shopping sprees anymore. Now thieves are using your personal info (or your child's) to get a job, buy a house, and have major surgery — which wrecks not just your bank account but also your medical records.

When her labor pains began last April, Dorothy Bell Moran, a troubled 28-year-old, showed up alone at Alta View Hospital in the Salt Lake City area. As identification, she handed over a driver's license. It wasn't hers, but Moran looked enough like the woman in the photo — young, with long dark hair and a toothy smile — that no one questioned her.

Moran was only 33 weeks pregnant, so she was taken to nearby University Hospital, which is better equipped to handle preemies. When she refused to pronounce her name at the intake desk, the sympathetic clerk assumed it was because she was in so much pain. Moran gave birth to a daughter without any friends or family around. Several days later, when the hospital ran tests, the baby girl came up positive for methamphetamine. But doctors couldn't talk to Moran — at some point, she had walked out of the hospital, leaving her newborn behind.

Soon after the baby's tests came back, Anndorie Sachs, 28, a biomedical engineering student who lives in Salt Lake City with her husband and kids, received a call from the Utah Division of Child and Family Services (DCFS). Your newborn, the investigator said, tested positive for drugs. "What do you mean?" Sachs recalls saying. "I didn't just have a baby." The agent's response: "Don't try to pull that with me!" She notified Sachs that DCFS was ready to put through paperwork to take custody of Sachs's four children, then ages 2 to 7.

Sachs connected the dots right away: Two months earlier, someone had stolen her driver's license from her car. Remembering that, she called her husband, a contractor, who sped home from work.

As the couple was sitting in their living room anxiously awaiting the agent, their 7-year-old daughter, Sierra, was being pulled from her first-grade classroom. The DCFS agent asked the girl if her mother had been in the hospital recently. Sierra answered yes, and proudly showed off the spot on her arm where a nurse had inserted an IV. (She'd had an infection several days earlier.) Then the investigator asked Sierra if her mom had a new baby. The little girl said no. And, no, her mother had not been away for the past few days.

When the DCFS agent finally arrived at the house, she could see that Sachs hadn't given birth recently. But she still needed proof that this wasn't the woman who had abandoned an infant in a hospital and racked up a \$10,000 bill. "It took five full minutes," Sachs recalls, "before she started to believe what I was saying."

The accusations were dropped and Sachs was cleared of paying Moran's hospital bills, but the ordeal wasn't over. Sachs's medical records had been altered to include the blood type and general health record of a complete stranger. The two hospitals assured Sachs that they'd fixed the problem, but she can't be 100 percent sure because — in a catch-22 of utter insanity — they wouldn't let her see her own records, lest *Moran's* privacy rights be violated. "It's especially scary," she says, "because I have a blood-clotting disorder. If a doctor gave me the wrong blood type, it could be fatal."

Target: Your Insurance Card

Using someone else's name to get health care is known as medical identity theft, and it's a growing headache for hospitals and insurance companies — and, worse than that, for the approximately 200,000 Americans who will become victims every year, the Federal Trade Commission (FTC) estimates.

This scam comprises only about 2 percent of the total ID theft cases reported annually to the FTC. But it's

"a sleeper that's starting to awake," says Kirk Nahra, a Washington, D.C., lawyer who chairs an American Bar Association group addressing the issue. "As health-care costs continue to go up," he says, "people will try to get help without paying for it."

Many reported cases like Dorothy Moran's are individual crimes of desperation. Others are more calculated inside jobs, according to a 2006 report by the World Privacy Forum. Last year, for example, a receptionist at the Cleveland Clinic Florida in Weston, FL, secretly copied the medical records of more than 1,100 people. Then she sold them to her cousin, who ran a medical clinic in Naples, FL. He billed the patients' insurance for a multitude of tests and procedures — making the people appear much sicker than they really were — so he could cash in. In total, he collected \$2.8 million.

"Can you imagine if, say, HIV were put into your records erroneously?" says Pam Dixon, executive director of the World Privacy Forum and author of the report. She says victims often aren't aware of errors until months or even years later, when they're denied coverage or are informed that they've maxed out their insurance.

How do thieves cover their tracks? "Typically, with these inside cases, the first thing they do is change the address on the insurance form, so you never receive an explanation-of-benefits letter," says Dixon. "So if you ever stop getting those notices, be alarmed."

While victims of financial ID theft can restore their credit records, there are no guidelines in place for this scary new type of fraud. Medical records are scattered among providers, so they're hard to correct. Sachs learned this the hard way. Several months after the Moran incident, she came down with a kidney infection. "I didn't want to deal with any mix-ups," Sachs explains, so she sought treatment at a different local hospital. Yet when a staffer opened her patient profile, Sachs saw that people in Las Vegas were listed as her emergency contacts — even though she has no friends or relatives there. University Hospital eventually did allow her to review her records, and she saw no major errors. But when she asked to check her file at Alta View, several hospital representatives told her they could find no record of her in the system — even though she had been a patient there before the Moran episode. The bottom line: She has no way of knowing how many Las Vegas-like errors may have found their way into the vast database of electronic records.

The repercussions of medical ID theft go beyond hospitals. More than one-third of Fortune 500 companies now demand to see medical records before making hires. "There are people who cannot get a job or insurance because their records say they have MS, HIV, or some other illness that they don't really have," says Dixon. "These people are tagged with conditions that make them uninsurable."

Moran has managed to avoid paying a major price for her actions. Charged with identity theft, she accepted a plea bargain and last fall, was sentenced to drug treatment and three years' probation in return for pleading guilty in a separate, unrelated case. Charges in the Sachs case were dismissed and the baby, who had been in foster care, was eventually returned to her mother.

Today, Sachs feels a mixture of anger and pity. "Mostly, I feel sorry for the baby," she says. "I keep reminding myself that she's the bigger victim." (DCFS reported at press time that the child was with Moran in a residential drug treatment center and that both were doing well.)

Target: Your Social Security Number

For as little as \$20, you can purchase a fake Social Security card. At ID mills around the country, buyers receive a reasonably authentic-looking card with their name and a nine-digit number. The seller generates the number on the card — but in most cases, by chance, that number already belongs to someone else. The person may be deceased or alive and unaware, age 4 or 84.

In Utah and Houston, where many cases of Social Security ID theft are in the courts, prosecutors say that a majority of imposters are illegal immigrants (such as Betty's father on the TV show *Ugly Betty*). There are no national statistics.

"Some immigrants cross the border, go to an ID mill, and say, 'I need an SS card and this is the name I want on it,'" explains Houston Assistant District Attorney John Brewer. "They get jobs, start working, and eventually — when they realize they're not going to get caught — grow more comfortable with the number. Then they go the next step and sign up for a car loan or mortgage."

And they usually get away with the crime because there are surprisingly few checks to stop this kind of theft, say prosecutors: Employers aren't required by law to verify Social Security Numbers and some car

salesmen and mortgage brokers are willing to overlook a fishy credit report in order to complete a sale.

Every year, the Social Security Administration (SSA) receives eight to nine *million* earnings reports where the name doesn't match the SSN. Sometimes it's a minor mix-up — there are women, for example, who get married and change their names, but never notify the SSA. In a growing number of cases, however, the problem is ID theft. And the perpetrators rarely get caught because wage reports (like medical files) are considered private. So when a mismatch occurs, instead of investigating, the SSA places the suspect documents in a "suspense file" and essentially walks away.

For example, the SSA never told one victim in Utah that her number had been stolen by an illegal immigrant named Araceli M. Lagunes. If Lagunes's victim had ordered a credit report, would she have discovered that an ID thief used her number to get a mortgage (and refinance it at least once)? Not necessarily. Because Lagunes was using her own name, not her victim's, Lagunes's credit history went into a subfile, completely separate from the victim's (though linked by their shared number). However, Lagunes's credit activity could be seen by any merchant or employer who ran a check on the card. Worse still, Lagunes's bill-paying habits, whatever they were, could have affected the rightful owner's credit score. (Lagunes has pleaded guilty.)

"This is a kettle that's about to boil over," says Utah Assistant Attorney General Richard Hamp. "The federal government won't lift the lid off." Hamp, one of the few attorneys general devoted to uncovering and publicizing this type of case, discovered that 132,000 SSNs were being used by more than one person in Utah alone in 2000.

In Houston, a city that ranks fourth in reported cases of identity theft per capita, Brewer is now pursuing the ID mills that brazenly sell fake cards, arguing that they promote other kinds of illegal activity. "The people who use these numbers are officially not on the grid," he says. "That has implications for safety and terrorism."

The real problem is that only a tiny fraction of SSN victims are even aware of the theft. If the imposter regularly pays his or her bills on time, the crime is uncovered only by the better credit monitoring services. In other cases, the fraud is exposed by sheer chance, as in the case of Grace Weed.

Grace was just 5 years old when her parents learned her SSN had been stolen. As she entered kindergarten last year in Magna, UT, her father switched jobs. Since his new health insurance wouldn't kick in for a few months, he and his wife, Lynette, enrolled Grace and her older brother in a state-run insurance program for children. Not long afterward, Lynette Weed received a call from an insurance administrator, who said Grace's SSN showed income earnings, which would disqualify the girl for aid. "She implied that if I was using Grace's number, I'd better stop," says Weed, who owns a beauty salon. (Some parents fraudulently use their children's numbers when their own credit record is poor. Illegal immigrants whose children are born in the United States have also been known to use their kids' numbers.) "She could tell by my surprise that I wasn't doing anything wrong. Then she said, 'Someone must have stolen your daughter's number.'"

Weed called the attorney general's office, filed a police report, and learned to her astonishment that at least 10 people (or someone with 10 different aliases) were using Grace's number — some since 2002, the year after her birth.

Knowing that there were 10 imposters operating in a state with only one major metropolitan center, Weed wasn't surprised when she got a call from the billing department at the eye, ear, nose, and throat specialists where Grace had been a patient. At their Park City office, they had turned away a man who had given Grace's SSN as identification. "I thanked the receptionist and said, 'Please call the police and the attorney general.'"

After the Weeds reported the Social Security theft, there was little else to be done about the problem. The SSA refused to issue Grace another number. (According to an agency spokesperson, a new number may be issued if a victim "continues to be disadvantaged by using the original number." Because she was still a child, Grace hadn't faced any problems and thus presumably could not be given a new number.) A spokesman for Experian, one of the three national credit-reporting companies, insists that Grace and the imposters will remain separate in their computer files. If that were the case, she would have no trouble getting student loans down the line.

Experts say that this forecast is far too sunny. If someone is using your SSN, the system is supposed to register at least one other shared piece of data — a name, address, or birth date — before the thief's information shows up on your credit report. "The problem is that credit-bureau merging software makes

mistakes, and even if you share just the SSN with another person, that could be enough to trash your credit," explains Edward Jamison, a California attorney who specializes in credit matters. "It's not a perfect system."

The Weeds expect a lifelong battle with Grace's number. But there has been progress. Lynette Weed said that two men who have used Grace's number are currently being investigated; if prosecuted, they could face a fine and possible prison time. "If there are court hearings, I plan to attend with Grace," she says. "I want to show these men that there was a real person attached to that number, a little girl who's going to have to clean up their mess later on."

How to Detect and Prevent ID Theft

The first step is simple: Get a free annual review of your family's credit reports. Here, seven other helpful tips


Medical ID Fraud

- Protect your insurance card as carefully as your credit cards. If it gets lost or stolen, alert your insurance company immediately and request a new number.
- Be selective about where you get care. Avoid clinics that advertise free exams; they may just want to copy your health insurance information.
- Carefully read over the explanation-of-benefits notices that your insurance company provides. Make sure you recognize the doctors' names and the dates of treatment — an unfamiliar provider is a big warning sign. If you rarely see your doctors, call your insurance carrier and ask for an annual summary of all procedures that were paid in your name.

Social Security ID Fraud

- Use a credit monitoring service (roughly \$11 per month), which notifies you within 24 hours if there's unusual activity. Identity theft expert Frank W. Abagnale, author of *Catch Me If You Can* and *Stealing Your Life*, recommends PrivacyGuard, Equifax Credit Watch, and Identity Guard.
- Before you toss sensitive financial documents and those credit card solicitations that come in the mail, destroy them in a micro-cut shredder.
- Don't give out your SSN freely. "There's no reason the storage center or the dog pound needs to know your number," says Abagnale.
- Never answer unsolicited phone or e-mail messages about your accounts, even if they sound or look legitimate.

Find this article at: <http://www.goodhousekeeping.com/id-theft-0807>

 Click to Print

[Close](#)
