

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 *continued on page 162*

How to Detect and Prevent ID Theft

The first step is simple: Get a free annual review of your family's credit reports (visit Annualcreditreport.com or call 877-322-8228). 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.

