

# NEWS&TRENDS

## Stealing Your Life

### Identity Thieves Hit Nearly 10 Million Americans Last Year— Could You Be Next?

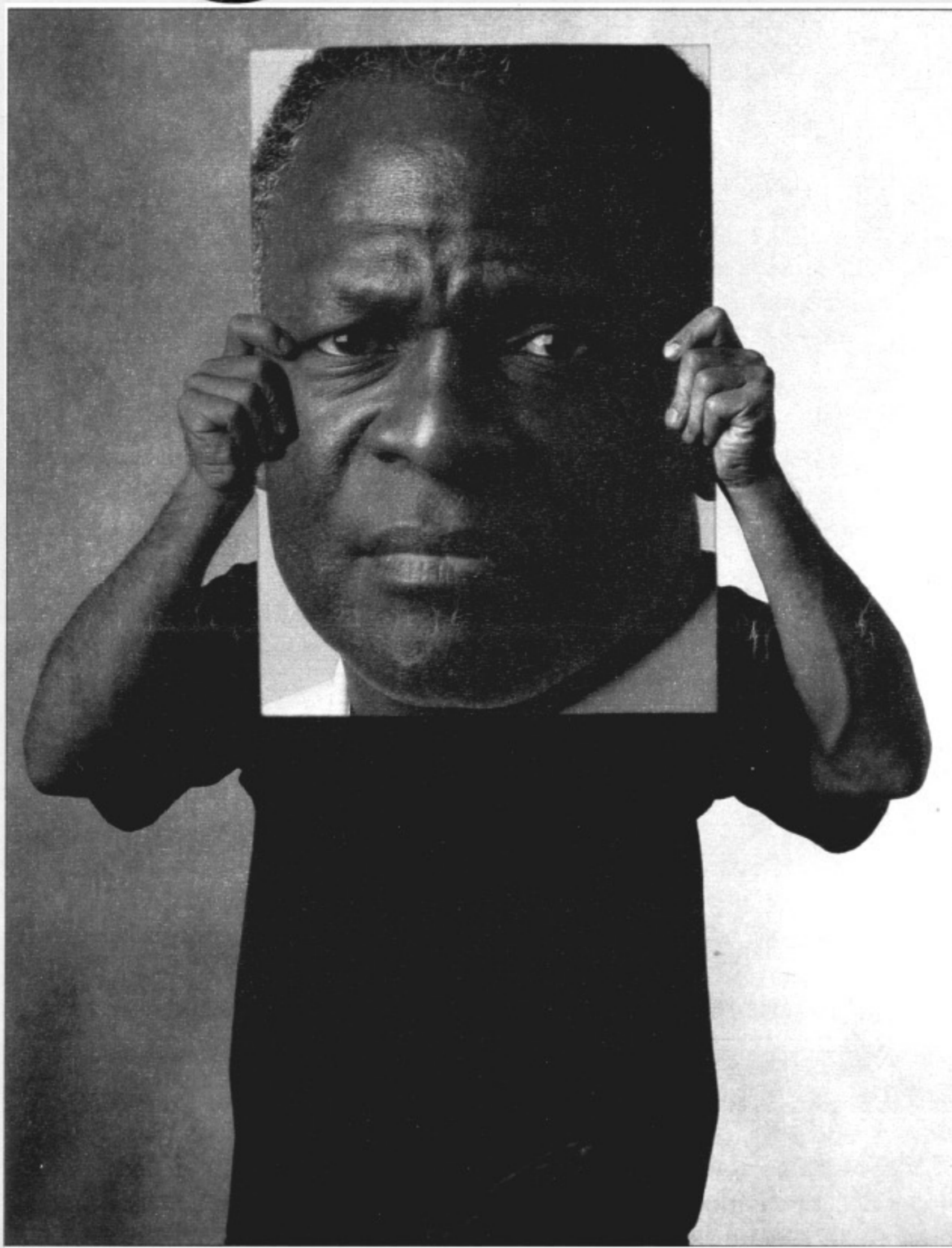
BY CAROLE FLECK

It's a shattering violation of privacy, a near-perfect crime—and most victims don't even know they've been robbed until it's too late.

If you think it can't happen to you, think again. Last year nearly 10 million Americans were victims of identity theft, the fastest-growing crime in the country. And there's no end in sight: Experts say the number of cases has been doubling every year since 2000.

For perpetrators who are clever enough to move quickly from victim to victim, identity theft is a high-profit, low-risk and—until recently, at least—low-penalty type of robbery. And most of these impostors are never caught.

The crime can take many forms but always involves the misappropriation of names, Social Security numbers, credit card numbers or other pieces of personal informa-



tion for fraudulent purposes.

"If you have a bank account, you're vulnerable," says Cynthia Oberg, an assistant United States attorney in Detroit who's prosecuted many identity theft cases. "I don't think there's anything you can do to completely protect yourself against it."

Just ask Kathleen Cox, 82, of Rockville, Md. She endured what she calls "one and a half years of hell"—complete with medical bills and lawsuits that should have been directed at someone else—after a woman passed herself off to police as Cox following a four-car collision. [See box below.]

Or consider the case of John Harrison, 42, a retired Army captain in Rocky Hill, Conn. An identity thief armed with a fraudulent military ID card acquired goods, services and cash valued at more than \$260,000, including two trucks, a \$25,000 Harley-Davidson motorcycle and a time-share vacation place in Hilton Head, S.C. After the thief wrote bad checks in his name, Harrison's military retirement pay was garnished.

"It has been and continues to be a nightmare," Harrison told members of the Senate Banking Committee last year. Soon after, Con-

CONTINUED ON PAGE 4

### One Woman's 'Living Hell'

Kathleen Cox, an 82-year-old grandmother in Rockville, Md., quit driving during the Truman administration. But in 2001, Cox suddenly found herself in what she describes as "a living hell" after one of her neighbors, arrested on drunk-driving charges in Illinois following a four-car collision, pretended to be her.

Cox first suspected something was amiss when she received bills totaling \$9,000 from a hospital in

Illinois that had treated the impostor's injuries. Then she received a summons notifying her that a woman hurt in the accident had filed a \$50,000 lawsuit against her. "I was told there were warrants out for my arrest," says Cox, who writes children's books. "I was afraid to answer the phone."

Cox says police refused to investigate—a complaint echoed by many identity theft victims. So she did the investigating herself. Soon she learned that the identity thief shared her name—a twist that made much

of the fraud more difficult to resolve.

Police finally caught up with the impostor, and most of Cox's troubles are behind her. But there's still one more wrinkle in her ordeal.

"She's due in court next week," Cox said in January of the other Cox, "but she never gets the notices, the summons, the threats. I do. They keep sending them to my address."

Cox adds, "It's an awful way to live. I've had enough heartache over it."

## NEWS&amp;TRENDS

## ID THEFT

CONTINUED FROM PAGE 3

gress passed the Fair and Accurate Credit Transaction Act to slow the rising tide of identity theft.

In an interview with the *AARP Bulletin* Treasury Secretary John Snow praised the law, which will take effect in December.

"It gives people access to their credit reports," Snow says. "It requires financial institutions to be ... alert to the patterns of identity theft."

Many victims don't even realize their identities have been hijacked until they see mysterious charges on their credit card bills, they're turned down for credit or they get harassing calls from debt collectors.

According to the Federal Trade Commission (FTC), 38 percent of all identity theft victims spend more than a month—and often much longer than that—to figure out what's happened to them.

By then, more often than not, their credit is wrecked. Even worse, they may be sought by the police for crimes committed in their name.

David Szwak, a lawyer in Shreveport, La., who's represented scores of identity theft victims, calls it "an epidemic of monumental proportions," adding that "any moron can do it and get away with it." And get away with it they do. Although the person who stole Harrison's identity is now behind bars, that's the exception.

Linda Foley, founder of the Identity Theft Resource Center, a San Diego-based nonprofit group, estimates that only one in 20 acts of identity theft ends with an arrest of the offender.

"Identity theft is a growth industry," Robert Gellman, a Washington privacy consultant, told the *Bulletin*. "The marginal [enforcement] efforts don't touch the scope of the problem."

The FTC, in fact, estimates that identity thieves last year cost consumers \$5 billion in out-of-pocket expenses and businesses \$48 billion.

"There isn't anything they can't do in someone else's name," says Betsy Broder, an identity theft expert with



**Identity theft is 'an epidemic of monumental proportions. Any moron can do it and get away with it.'**

### To Stop a Thief

**Seal your lips.** Never give your Social Security number—or personal information of any kind—over the telephone or online unless you initiate the contact.

**Shred.** Shred bank and credit card statements, canceled checks, preapproved credit card offers, bills with account information and the like.

**Guard your mailbox.** When you pay bills, don't put them in your mailbox with the flag up. Use a locked mailbox or the post office.

**Check your credit reports.** Look for telltale markers of identity theft, say, an address change you didn't make or new account you didn't open.

Cancel accounts you don't use or only rarely use—open credit is a prime target.

**Scrutinize bank statements.** Monitor your accounts frequently for suspicious activity. And don't have blank checks mailed to your home; pick them up at your bank instead.

**Be careful at ATMs.** "Shoulder surfers" can get your account and PIN numbers.

**Build a firewall.** If you use a computer at home, protect yourself by installing firewall software.

**Memorize.** Don't write down PIN numbers, passwords and the like—commit them to memory.

the FTC. "They're able to get the equity out of your house, they're able to buy luxury cars in your name, they've evaded law enforcement by using someone else's name when they're arrested. They're resourceful and creative."

Indeed. James G. Huse, the inspector general of the Social Security Administration, tells the story of a San Diego man—a fugitive felon for 17 years—who, using the Social Security number of a 70-year-old South Dakota woman, created 33 different identities with fraudulent documents. The fugitive used the stolen identities not only to avoid capture but also to get such jobs as head of security for a county fair and chief of a fire department.

Older people often are attractive targets for identity thieves, experts say, because they tend to have accumulated more savings via paid-up mortgages and Social Security checks and have flawless credit.

"People over age 50 control at least 70 percent of the nation's household net worth," Huse says.

### FAULT LINES

Identity thieves can purloin information just about anywhere—from receipts at stores, restaurants and ATM machines, from personnel files, medical records and even mail containing Social Security numbers tossed into a trash can.

Such ready access fuels the explosion of the crime. So do some other factors:

- **The wholesaling of personal data.** Thanks to technology, information on millions of Americans is stored in computer databases—mammoth and largely unregulated repositories that are potential gold mines for thieves.
- **The expansion of e-commerce.** Criminals use the Internet to make purchases in their victims' names—without risking face-to-face contact.
- **Ubiquitous, everyday invasions of privacy.** Businesses collect too much information. "Why does the vet need your Social Security number?" asks Foley of the Identity Theft Resource Center.

• **Careless caretaking of sensitive data.**

Some institutions do a poor job of protecting personal data. Beth Givens, founder of the San Diego-based Privacy Rights Clearinghouse, cites the workplace in particular as a breeding ground for identity theft. "It's quite lucrative," she says. "All it takes is one dishonest employee to collect data on thousands of employees."

• **The proliferation of "instant" credit.**

The nation's retailers often issue credit on the spot, experts say, and fail to properly verify the identities of applicants. Too often, they add, retailers even ignore fraud alerts that consumers have placed in their own credit files.

"Credit granters like department stores are so desperate for business that they give instant credit, and [the criminal] walks out the door with five projection TVs in someone else's name," says Gellman, the privacy consultant. "It's a big part of the problem."

**IS ANYTHING BEING DONE?**

Victims of identity theft spend an average of 175 hours and up to \$1,000 trying to undo the damage—or at least straighten out the mess—that's

part and parcel of the crime.

Even with the help of a lawyer, it took Melvin and Loretta McBride of Fort Worth, Texas, seven years to get their financial life in order after an identity thief opened 12 credit cards and ran up \$100,000 in charges in their name. Among other things, the ordeal sank their efforts

to refinance their home mortgage at a lower interest rate.

"You go along your whole life and you pay your bills and you try to do the right thing," Loretta McBride, 73, told the *Bulletin*. "The upheaval and the worry—it was nerve-wracking."

The new legislation Congress passed, after years of hearings, gives

people new tools to defend against identity theft. Consumers will be able to get a free credit report every year to review for any unauthorized activity. Merchants will be required to delete all but the last five digits of credit card numbers on receipts.

The law allows victims of identity theft to trigger a nationwide fraud alert with a single telephone call to one of the three top credit bureaus.

But some consumer organizations have criticized the law for preempting tougher state laws and for failing to give consumers enough control over how companies use their financial information.

"Without tougher financial privacy laws," says Rob Schneider, director of Consumer Union's FinancialPrivacyNow.org project, "consumers will remain vulnerable to identity theft, aggressive marketing and fraud."

Even so, Treasury Secretary Snow, who was at President Bush's side when he signed the law Dec. 4, called it "a beginning" in the government's battle against identity theft.

"But," he adds, "individual responsibility plays a critical role. Vigilance is key." ■

**The workplace is a breeding ground for identity theft. It only takes one dishonest employee to get data on thousands of others.**

**To Learn More About Self-Defense**

The Federal Trade Commission (FTC) offers a wealth of information about identity theft at [www.consumer.gov/idtheft](http://www.consumer.gov/idtheft).

Other useful sites:

- FBI's Internet Fraud Complaint Center, [www.ifccfbi.gov](http://www.ifccfbi.gov).
- Identity Theft Resource Center, [www.idtheftcenter.org](http://www.idtheftcenter.org).
- Privacy Rights Clearinghouse, [www.privacyrights.org](http://www.privacyrights.org)

For a copy of the FTC's free booklet, "ID Theft: When Bad Things Happen to Your Good Name," go to [www.ftc.gov/bcp/online/pubs/credit/idtheft.htm](http://www.ftc.gov/bcp/online/pubs/credit/idtheft.htm). Call AARP at (888)

687-2277 for a shorter version, "ID Theft, What's In It For You?" Ask for stock number D18052.

If you suspect identity theft, contact the credit reporting agencies and place a fraud alert on your accounts:

- Equifax, (888) 766-0008 or [www.equifax.com](http://www.equifax.com).
- Experian, (888) 397-3742 or [www.experian.com](http://www.experian.com).
- TransUnion, (800) 680-7289 or [www.transunion.com](http://www.transunion.com).
- File a police report.
- Complain to the FTC at (877) 438-4338.