

IDENTITY CRISIS

TARGETING INSTITUTIONS...

Each year, 7 million to 10 million Americans fall prey to identity theft—and the majority of them have never met the culprit. From massive data-brokerage firms to tiny local banks, your identity is irrevocably “out there.”

WHO ELSE HAS IT

Why the recent rise in major heists?

Blame it on “third party” players, who now have more access to your financial information and related data than ever before. Here’s where ID thieves go to get the goods on you:

- > Your bank, school, employer and doctor
- > Local DMV offices
- > Federal agencies (FDIC, DOJ, IRS)
- > Phone companies
- > Merchants
- > Card networks
- > Credit-reference agencies
- > Data-brokerage firms
- > Payment-processing agencies

HOW IT'S STOLEN

Security is lax and identity crooks are cunning. Some recent cases:

HACKING

DSW: In April, the shoe chain revealed that hackers had stolen data from 1.4 million credit- and debit-card transactions at 100 stores in 25 states. The breach also included account numbers from 96,000 check transactions.

Exposed: **1.5 million**

CardSystems: This processing agency improperly retained info on credit-card customers for research. When hackers hit its system in May, it was the biggest data breach in U.S. history.

Exposed: **40 million**

CONS AND SCAMS

Bank of America/Wachovia: Working with upper-level employees in April to identify vital customer info, a middleman allegedly hawked credit-card and account numbers to outsiders.

Exposed: **676,000**

ChoicePoint: Last year it sent thousands of reports stocked with names, SSNs and financial info to con artists posing as legit debt-collection, insurance and check-cashing businesses.

Exposed: **145,000**

YOUR DATA

Your real fingerprints aren't etched on your fingertips; they're stored on computers and printed on paper and plastic. What ID thieves want:

- > Credit-card numbers
- > CW2 security numbers (on back of credit card)
- > Credit reports
- > Social Security number
- > Driver's license number
- > ATM cards
- > Telephone calling cards
- > Mortgage details
- > Date of birth
- > Passwords/PINs
- > Home address
- > Phone numbers

... AND YOU, TOO

Stealing wallets is *so* 1995.

Today, identity thieves rely on a variety of tactics (both high- and low-tech) to pick your pocket. A look at the most popular—and effective:

'Dumpster diving': Rifling through trash bins—home, office, public—for loan applications, credit-card documents and any printed Social Security numbers.

'Shoulder surfing': Lurking at ATM machines or phone booths to pick off PINs, credit-card numbers or passwords.

'Skimming': Stealing credit- or debit-card numbers by attaching a data-storage device to an ATM machine or the card reader at a retail checkout terminal.

'Phishing/pretexting': Posing by e-mail or phone as a legit company and claiming there's a problem with your account.