



Employment records prove ripe source for identity theft

By Stephanie Armour, USA TODAY

Confidential employment records might not be as secure as many employees assume they are. Job applications, personnel records and other employment data that should be safely filed in company offices or computers are instead being taken by thieves who use the information to steal workers' identities.

It's a maddening crime that's becoming more common. Information from personnel records are being used to rent apartments, carry out crimes, establish credit card accounts and buy cars. Some victims have been forced to legally change their names; others have spent years trying to untangle the credit damage.

As the crime mounts, federal agencies are trying to ratchet up awareness. Victims' rights groups, irate about the lack of protection provided by companies, are lobbying state legislatures to pass laws protecting records. More hapless employees are finding their financial lives devastated by an ID thief, who typically got access to data because he or she worked on the inside.

All kinds of information have been used for identity theft. Employees have tossed credit card receipts from business lunches into the trash only to have cleaning staff take the information. CEOs have been victimized by managers they fired. Employees who get company credit cards have had their information stolen by employees of the vendors that provide the cards.

"You can't really protect yourself," says Martha Steimel, president of Washington-based Victim's Assistance of America, which focuses on identity theft. "Anybody who has access to employment files can turn you into a victim. You can be totally mutilated financially by an identity theft perpetrator. It's scary."

This is no phantom risk.

- In a report released Wednesday, the Federal Trade Commission said complaints about identity theft nearly doubled in 2002, accounting for 43% of consumer fraud complaints and leading a list of consumer frauds for the third consecutive year. The number of consumer contacts the FTC received regarding identity theft ballooned from 3,350 a week in December 2001 to 4,655 a week during December of last year.
- The top cause of identity fraud is now theft of records from employers or other businesses that have records on many individuals, according to a 2002 report by

credit information provider TransUnion. That beats all other sources, including stolen credit cards, mail theft and stolen purses or wallets.

- And about 90% of business record thefts involve payroll or employment records, while only about 10% are customer lists, the FTC says.

Denise Heilig of Arlington, Tenn., says her identity was stolen at a previous workplace. The perpetrators set up credit card accounts in her name, and it took numerous police reports and months of work to sort out the mess.

"It was a horrible time for us," says Heilig, 37. "Companies should be held accountable for this. They want to protect their assets, but they won't protect us."

Workers can't do much about it

There's little employees can do on their own to keep records safe. There are myriad ways to get the information needed to carry out an identity theft. Often, Social Security numbers, addresses and other data are kept in paper files or on computers. Anyone who has access to those files, either online or otherwise, has the means to carry out an identity theft. Often, the thief is a fellow employee working for human resources, payroll or another department with access.

There are other methods:

- Thieves sometimes take jobs as temporary workers to get into a company so they can nab employee data.
- Others work for third-party vendors that do business with a company, such as handling corporate credit accounts or providing janitorial staff.
- Sometimes, the information is stolen by a colleague from a co-worker's purse.
- And in some cases, companies use ID badges that are actually employees' Social Security numbers — meaning anyone seeing the badge has what is needed to carry out an ID crime.

When a theft happens, companies' reactions vary. Some don't know a crime has taken place until employees start getting calls and credit bills. Others wait to alert employees, a stance that angers victims' rights advocates who are pressing for legislation requiring companies to inform workers when data has been taken.

Only as awareness mounts are some companies taking steps to protect data. They're locking up paper files, keeping audit trails to document who has reviewed employment data, removing Social Security data from IDs and bringing in third parties to carry out privacy investigations that gauge how vulnerable records are to theft.

Some union groups are calling for more action, especially following recent thefts.

More than 40 workers at Woodbridge, a factory that makes foam for car seats in Brodhead, Wis., became identity theft victims. Tens of thousands of dollars in bogus

credit charges and phone bills have been amassed since May 2001 in their names, and union members are pressing for better safeguards on personnel data.

"I've seen the frustration they've had to go through," says Janet Cook, president of the Union of Needletrades, Industrial and Textile Employees Local 1871. "Whenever they want to buy something, they have to prove who they are again and again."

Woodbridge company officials could not be reached.

ID theft increasing

The crime of ID theft using employment records is growing for several reasons. Blame it on more use of technology to store employment data, which means all it takes, is a few keystrokes to get access to hundreds or thousands of workers' records. In addition, the sluggish economy might be driving more people to commit such theft, crime experts say.

"Most businesses think of client records as the most valuable, but payroll records are more often than not what are stolen," says Joanna Crane, program manager of the FTC's identity theft program. "It's happening with increasing frequency."

Most companies do little to protect employment data, but even those that try to take precautionary steps have fallen victim.

At Arkansas Children's Hospital in Little Rock, officials say steps have long been in place to protect personnel data. The hospital runs audits on computerized information on who has access, conducts background checks on employees and temporary workers, and carries out both drug tests and random drug screens.

Even so, two temporary workers were charged in 2002 with stealing information from employee records: They allegedly took the names, birth dates and Social Security numbers of hospital pharmacists. Police say the two and an accomplice who hadn't worked at the hospital used the data to set up charge accounts at Best Buy, Home Depot and other stores.

The case has yet to go to trial. Police say about six employees were victims, losing a total of at least \$10,000. And the hospital wasn't alone, police say. The identity theft was part of a broader operation, they say, where the identity thieves worked as temporary hires to get access to personnel records.

"They sought out jobs through temporary agencies where they would have access to the information," says Andree Trosclair, vice president of the hospital's human resources department. "People look at (human resources) like we've done something wrong. You do a lot, but there's only so much you can do. We take confidentiality and privacy very seriously."

But victim advocates say most companies are doing woefully little to protect employee data that can be used by identity thieves. Many are unaware that such slapdash practices can put workers at risk, while others don't believe it's their responsibility to protect the data.

Says Mari Frank, author of *The Identity Theft Survival Kit*, on restoring credit and surviving the crime: "The way businesses handle information is often very careless, and there are a lot of dirty employees. It's scary."

Developing safeguards

That lack of attention to identity theft risks in the workplace is starting to change, however. Some states, such as Georgia and Wisconsin, have passed laws requiring employers to destroy documents containing personal employee data. California passed legislation barring private firms from using Social Security numbers as identification numbers.

In April, the FTC convened its first workshop for businesses on safe record keeping, and the agency is working with industries to develop best practices.

Companies also are starting to revamp policies as workers who've been victims sue employers for negligence. Last year, Ligand Pharmaceuticals in San Diego settled a lawsuit brought by some employees who were victims of ID theft.

After Ligand merged with another company, personnel records on some of the acquired company's workers were kept in a storage area, lawyers say. An employee found the box and used such data as names, birth dates, addresses and Social Security numbers to rack up credit card bills and rent apartments, lawyers say. More than 30 employees were victims.

Some sued Ligand for negligence, claiming the company had not taken enough care of their personal information.

A spokesman for the company declined to comment, saying Ligand has a policy of not speaking on litigation matters.

Such cases are setting off alarms. Identity theft wasn't considered a federal crime until 1998. Now, companies are beginning to take such defensive steps as privacy audits or removal of Social Security numbers from worker ID badges.

Last year, the then-governor of Illinois ordered a complete review of how employees' personnel information is kept.

"We'll use the information to assess and analyze different agencies," says Judy Pardonnet, a spokeswoman for the state's Central Management Services.

The edict came after an employee of the Human Services Department stole personnel data such as Social Security numbers from thousands of state workers, officials say. The information was used to open credit card accounts, and hundreds of thousands of dollars were charged in employees' names, officials say.

If a company doesn't take steps, workers who try to protect themselves often worry others see them as paranoid. Linda Foley says she became aware of how vulnerable employees can be after she became a victim of identity crime in the workplace. She says a past employer stole her employment data and racked up debts in her name. After her experience, Foley in 1999 founded the Identity Theft Resource Center to aid other victims.

"Afterwards, I didn't want to give my Social Security number on job applications," says Foley of San Diego. "Guess what? I didn't get job interviews. It was like, 'Why is she uncooperative? What kind of baggage do you have?' "