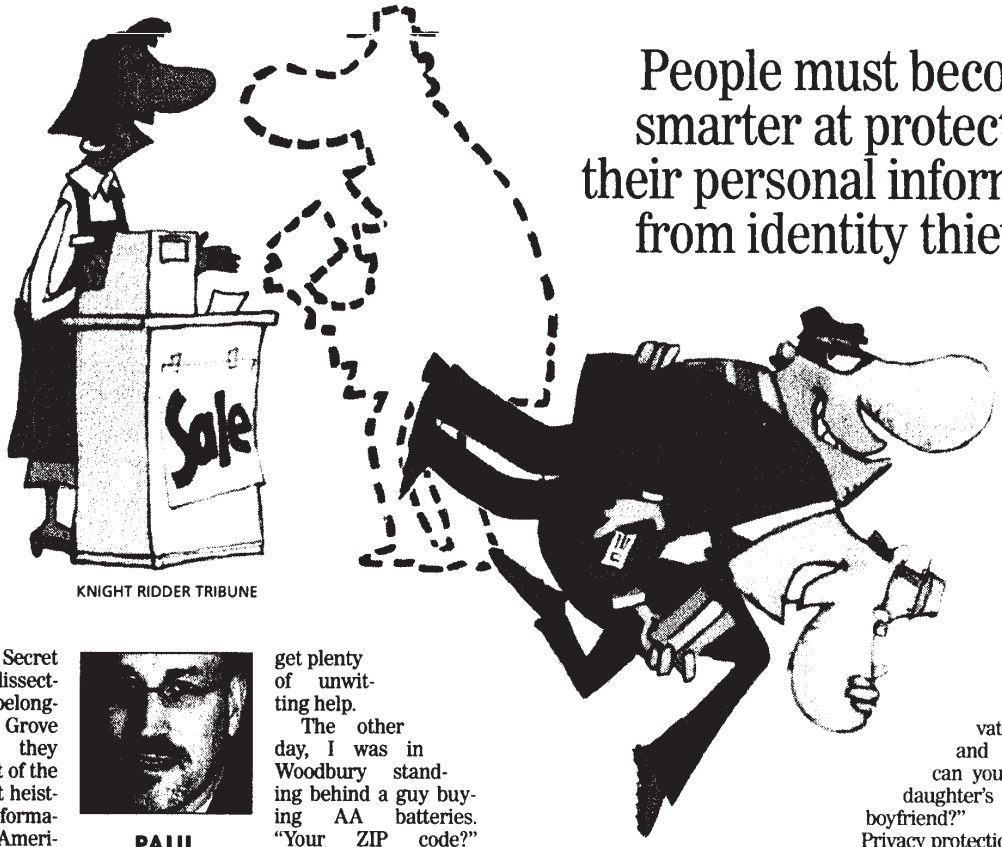
We're all vulnerable

People must become smarter at protecting their personal information from identity thieves.



KNIGHT RIDDER TRIBUNE

PAUL JAEB

The FBI and Secret Service are dissecting computers belonging to a Maple Grove teenager who they believe to be part of the ID theft ring that heisted personal information on 310,000 Americans.

The gang allegedly hacked into the e-mail account of a Florida police officer with access to database giant Lexis-Nexis. According to news reports, the officer mistakenly opened a junk e-mail armed with a virus that allowed the group to record everything he typed — including Lexis-Nexis passwords.

Personal identify theft is high-tech Mad Cow. The Federal Trade Commission estimates 10 million Americans a year fall victim to identify theft. Included this year are an estimated 2,000 Minnesotans whose personal information — along with that of 144,500 others across the country — was unwittingly sold to a California-based gang of serial identity thieves by ChoicePoint, a Lexis-Nexis competitor whose more than 50,000 clients also happen to include the FBI, CIA and Defense Department.

"The bad guys are very smart and very committed," ChoicePoint spokesman James Lee explained. He's right. But the bad guys also get plenty of unwitting help.

The other day, I was in Woodbury standing behind a guy buying AA batteries. "Your ZIP code?" asked the cashier. Battery Guy blurted out the numbers and then accepted her invitation to complete an instant credit application — for one of about 478 million retail credit cards now in use, according the Card Industries Directory.

A two-minute approval and he was good to shop. Never mind that the cashier had just extracted enough information to become Battery Guy. Or that she probably dropped the application form into an unsecured cardboard box for pick-up at the end of the day.

Now if the person who collects that application happens to be another Christopher Jones — the University of North Carolina-Pembroke employee who amassed 3,000 Social Security numbers while renting towels at the gym, and then attempted to sell them on eBay — a dead flashlight's going to be the least of Battery Guy's problems.

The ChoicePoint debacle has already spawned a new round of congressional hearings looking to tighten privacy regulations.

The laws may get tougher, but that, alone, won't solve the problem. The information services industry is already awash in regulation. The Fair Credit Reporting Act and the industry's own Individual Reference Services Privacy Principles cover almost every conceivable situation with a legal requirement or a best practices standard.

The devil is in the details. The Privacy Principles, for example, directed ChoicePoint to conduct a background check on the California cons. Sure enough, ChoicePoint did, and found them to be legitimate business people.

Why? Because the crooks — being crooks — had used stolen identities to apply for legal business documentation.

Second, when it comes to privacy protection, we are a bit hypocritical. Just recently, an audience member confronted me during an East Metro Rotary speech as I explained how investigators and police use Social Security numbers to nail deadbeat dads and lock away sex offenders. Nothing, she argued, could justify such Orwellian behavior.

Later, she privately approached and asked: "What can you dig up on my daughter's dirtball boyfriend?"

Privacy protection is like airport security. We are all for it — until we're late for the plane.

But post-Sept. 11, we recognize that government can't protect us unless we cooperate. So we unwrap computers, remove shoes and empty our pockets into plastic trays. In trade, hopefully, for a safer flight.

We need to adapt the same attitude about personal information. Before you share anything, stop and think.

Do I really need another credit account? Does it make sense to reveal my neighborhood ZIP code just to buy a pack of batteries?

Same as at the airport, government and law enforcement will do their best.

But same as terrorists, ID thieves will continue to threaten us until we all start practicing the privacy equivalent of taking off our shoes.

Jaeb is CEO of Heartland Investigative Group, a Twin Cities-based firm specializing in investigations, fraud- and abuse-prevention and executive protection.