

Ismat Mangla, May 2005

I was awarded a significant scholarship on the basis of this piece.

America's Identity Crisis:

The flourishing business of identity theft.

The wife of a police officer and mother of two is hardly the type of person you'd expect to be serving five years in a state prison.

Yet Web designer Tonie Hammond is one of 700 inmates at Lee Arrendale Prison in Alto, Georgia. Just a few years ago, Ms. Hammond spent her free time at her family's private cabin at Lake Lanier, Georgia's premier lakeside resort destination. Today, her daily routine consists of kitchen detail and para-military inspections every afternoon.

It's hard to imagine how a Web designer for a large telecommunications company pulling \$100,000 a year—much less a policeman's wife—could end up doing hard time amongst convicted murderers, thieves and other criminals.

But Ms. Hammond can explain it in one word: "Greed."

Greed, and \$2.5 million worth of fraudulent charges Ms. Hammond racked up as an identity thief. While her family was oblivious to Ms. Hammond's extra-curricular activities, she was employing her knowledge of computers to amass a not-so-small fortune.

It all began when Ms. Hammond opened a credit card account online, using a fake name and Social Security number. "It took like two seconds, and I had it," she told a TV station in South Carolina. That first effort spiraled into a series of almost addictive identity thefts. "I was able to tap into financial banks, to their data banks, and get information ... to take elsewhere online and set up accounts."

Ms. Hammond quickly learned that when it came to valuable data in corporate America, the security was lax—and the spoils were spectacular. Soon, she was opening accounts with banks and various online lenders. Next, she moved on to stealing financial information from her company's clients. "I would take federal ID numbers and set up bogus accounts through them," she said.

Her scam was almost perfect: No one suspected her, not even her family. It would have remained that way until one day Ms. Hammond slipped, using her home computer for one of her cons. After that transgression, she was tracked by authorities and eventually convicted.

But while Ms. Hammond is serving time for her crimes, the majority of identity thieves don't get caught. A recent survey by Gartner Research found that identity thieves have just a 1 in 700 chance of being caught, with some estimates as high as 1 in 1,000.

Scary stuff, considering that identity theft is America's fastest-growing—and potentially most crippling—crime. "Identity theft has increased exponentially since 1998, and it continues

unabated,” said Judith Collins, director of Michigan State University’s Identity Theft Crime and Research Lab.

The Federal Trade Commission reports that in 2003 (the most recent figures available), 10 million Americans were victims of identity theft. Such crimes cost consumers and businesses a total of \$55 billion in annual losses—the equivalent of the annual profits of General Electric, Citigroup, Microsoft, Pfizer and Wal-Mart combined.

“Identity theft has emerged as one of the dominant white-collar crime problems of the 21st century,” said Chris Swecker, assistant director of the FBI’s criminal division, in a recent Senate Judiciary Committee hearing. And the personal impact individual victims face is both financially and mentally devastating: “Our survey found that victims spent almost 300 million hours correcting their records and reclaiming their good names,” said FTC chairwoman Deborah Platt Majoras.

Conventional wisdom that emphasizes the importance of paper shredders can only take you so far, added Ms. Collins. “Unfortunately, consumers can do very little to protect themselves. Granted, some identities are stolen from mailboxes or dumpsters or online hackers who usually have ‘inside’ collaborators, but the majority of thefts are committed inside the workplace.”

The headlines corroborate the numbers. Recent security gaffes at major corporations have resulted in scores of missing valuable data. 4.2 million consumer records have been lost from shoe wholesalers (DSW) to money-center banks that tout security (Citibank), from employer personal record files (Time Warner) to data aggregators responsible for verifying credit information (ChoicePoint). [See table 1.]

Numerous security breaches at small businesses, major universities and hospitals compound the problem. Even renowned cybersecurity leader Carnegie Mellon University isn’t immune to the onslaught of identity theft. In April hackers accessed sensitive personal information belonging to 20,000 applicants, students and staff members.

And it’s likely that things could be even worse than we know. Much of the recent data theft disclosure is due to a 2003 California law that requires businesses to report significant security lapses to consumers. When pressed in Senate hearings, LexisNexis President Kurt Sanford and ChoicePoint President Douglas Curling admitted that security breaches occurring prior to the California law went unreported. Pending legislation in other states may follow suit.

“We are witnessing a freefall,” said Robert Siciliano, Boston-based security expert and founder of IDTheftSecurity.com. “Between 20 and 25 million identities have been compromised in the last year.”

While such figures are troubling, the fallout will be downright terrifying, said Mr. Siciliano. “When the results come in, when all the credit card numbers have been opened up, the loans have been granted, that’s going to be the story. Right now, we’re worried about the loss of data. But the accounts that open up as a result of this missing data is the real story.”

Experts warn that the identity theft epidemic leaves the United States vulnerable to a host of crimes and economic disasters. “For every human victim of identity theft, one and usually more businesses are also victims. Identity theft is undermining the economy of our country,” said Ms. Collins. “Second, in all acts of terror against the United States, including September 11, the perpetrators use stolen identities to conceal their whereabouts and activities. Third, most or all other crimes are facilitated using stolen identities, including retail, bank, credit card, telecommunications, wire and multiple other frauds.”

Siciliano doesn't mince words: “It's a direct threat to our national security and to our economy.”

So what can consumers do to prevent themselves from being targeted? Not much, according to Beth Givens, founder and director of the Privacy Rights Clearinghouse. “Data breaches like this point out there's really nothing an individual can ultimately do to prevent identity theft.”

And American companies are more and more vulnerable to such data breaches. A recent FBI/Computer Security Institute survey revealed that between 2000 and 2003, 40 percent of all companies confronted information snatches every year. But it's not just the geeky, basement-dwelling computer hacker businesses must worry about. Carelessness on the part of companies and thieving employees account for a large portion of identity theft. [See table 2.]

Tonie Hammond preyed upon two such weaknesses in the security chain. Her Web savvy enabled her to access “secure” financial information, while her insider access to company information allowed her to take advantage of sensitive information.

But whatever damage individuals do, company carelessness stings the most: Bank of America lost the backup tapes containing personal information for 1.2 million credit card holders. The unencrypted tapes were shipped via commercial air; they never made it to their final destination.

When it comes to solutions, ideas abound. Collins believes that industry self-regulation is the way to go. “The solution to identity theft involves a three-pronged approach: IT security, personnel security and work process security.”

Vermont Attorney General William Sorrell advocates for consumers having the right to place security freezes on their credit. “One thing that a number of the states are doing right now, which is very effective in terms of combating identity theft, is to be able to freeze access to your credit report. California, Texas, Louisiana and Vermont have those laws or they're about to go into effect,” he said.

But many experts believe self-regulation must coincide with legislation, because consumers can't protect themselves. “This is an issue the market can't solve by itself,” said Marc Rotenberg, director of the Electronic Privacy Information Center. “There are some things consumers can do, but we also have to be realistic. You can ask consumers to learn how to drive a car or wear seatbelts, but you can't ask consumers to evaluate how well the brakes are working. Consumers face similar challenges.”

Legislation carries bi-partisan support. Senators Arlen Specter (R-PA) and Patrick Leahy (D-VT) both attested to the problem in an April Senate Judiciary Hearing. “We do need federal legislation ... there needs to be uniformity as we approach an enormous problem of this sort,” said Mr. Specter.

“The normal market discipline of disgruntled consumers cannot save the companies from themselves,” added Mr. Leahy. Even ChoicePoint Senior Vice President Don McGuffey testified that his company favored some type of federal legislation to combat further debacles. [See table 3.]

Meanwhile, amidst the tempest surrounding identity theft, the identity thief herself is hard at work at the center of the storm, quietly filching personas and code numbers in order to make a quick buck.

Tonie Hammond was one such thief who couldn't resist the crime's enticing allure: “It was just too easy.”