You Own You

When identity thieves open an account in your name, it should be the bank's problem, not yours.

By Kevin Drum

In 1995, a freelance editor in Washington, D.C., named Anne Meadows began a five-year nightmare when she got a call from an alert employee of BellSouth, who warned her that she had become a victim of identity theft. A year earlier, she learned, thieves had stolen her name, address, and Social-Security number from a government office, and that was all they needed to go on a binge. They had created fake IDs, cashed a government check made out to her, and applied for credit at several establishments in Atlanta.

That's bad enough. But the story gets even scarier because at this point, Meadows did everything she should have done. She called every business the ID thieves had tried to scam and told them not to extend credit to the impostors. She called First Union National Bank and told them not to let the thieves open a checking account. Then she contacted all three of the national credit reporting agencies and had a fraud alert put on her record to prevent the thieves from obtaining credit elsewhere.

None of it did any good. First Union opened a checking account for the thieves anyway, and they then went on a check-writing spree through Atlanta. An oil company gave them a credit card. TeleCheck, a check verification agency, tagged *Meadows* as a deadbeat when checks in her name started bouncing—they refused to clear her name unless First Union called them, but First Union refused to help. This lack of cooperation from the credit industry meant the problem took years to resolve: In January 2000, almost five years after Meadows had first found out about the ID theft, a bank employee loudly turned down her application to open an account "because of all those bad debts you left behind in Georgia."

Today, Meadows's problems are mostly over, but she still shudders when she remembers the experience. "I've had my house broken into and my car broken into," she says, "but nothing compared to this. Nobody did anything about it but me, so I kept on being repeatedly victimized. I was guilty until proven innocent."

It's common knowledge that the problem of identity theft is growing out of control. Two years ago, the Federal Trade Commission estimated that one in every 25 Americans is a victim of identity theft each year, netting a cool $50 billion for the thieves.

The dynamics of the process are all too simple. First, the thieves steal enough personal information—usually just a name and Social-Security number will do—to apply for a credit card in someone else's name. They can get this information from any of the countless institutions, large and small, that have access to personal data: banks, credit reporting agencies, credit card issuers, government agencies, universities, even doctors' offices. They might use an insider who works there—sometimes they pose as temps—or hack into the office database. Alternatively, the thieves set up scams that ask people to sign a phony petition or provide their information to a telephone pollster "for our records." Sometimes they just steal information from people's wallets or trash cans. Then, the thieves wield this information to apply for credit cards or other forms of commercial credit, which they use for buying sprees on someone else's tab. Since the subsequent bills are sent to a phony address, the victims are unlikely to discover what's happened until the day they're denied a loan because of all those unpaid credit card bills. By then, their credit report looks like Anne Meadows's, or worse.

Identity theft would be much harder—and the costs to victims much lower—were it not for the carelessness of the credit industry and of other institutions that handle personal data. Many institutions that handle sensitive personal data don't do enough to keep it safe. This year alone, there have been widely-reported security breaches at Time Warner,

Kevin Drum is a *Washington Monthly* contributing writer.

Bank of America, and data-brokers ChoicePoint and LexisNexis, involving the loss of personal information about millions of people. There's probably little that can be done to prevent thieves from getting information from doctors' offices, or from people's wallets, but it's currently far too easy for them to get it from large corporations or from institutions such as government agencies and universities.

In addition, credit-card companies and other credit lenders—banks, oil companies, and department stores, among others—rarely exercise significant oversight before signing up new customers. So, when thieves apply for a new credit card using pilfered information, they are rarely turned down.

Finally, and most devastatingly, credit-reporting agencies routinely add negative information to credit scores without checking whether all those unpaid bills might have been the result of identity theft. And they're slow and uncooperative when it comes to correcting their mistakes.

The credit industry and other data-handlers behave as they do because in many cases, no one but the victim cares about identity theft. Despite the passage of ID theft legislation last year, institutions that handle personal data pay a very small price when that data is stolen. And when credit card companies and others offering credit fail to look adequately into applicants and end up extending credit to thieves, they also go largely unpunished.

For their part, the major credit-reporting bureaus—Experian, Equifax, and TransUnion—don't seem to care much about the accuracy of their credit reports. In fact, they actually have a positive incentive to let ID theft flourish. Like mobsters offering "protection" to frightened store owners, credit-reporting agencies have recently begun taking advantage of the identity-theft boom to offer information age protection to frightened consumers. For $9.95 a month, Equifax offers "Credit Watch Gold," a service that alerts you whenever changes are made to your credit report. Experian and TransUnion offer similar services. In effect, customers are being asked to pay credit agencies to protect them from the negligence of those same agencies.

One way to cut down on identity theft would be to require commercial credit-reporting bureaus to offer services like this to all their consumers for free. After all, the credit-reporting agencies are the ones who are failing to ensure that their reports don't unfairly penalize victims of ID theft. Roughly speaking, this is the European approach: Although implementations vary from country to country, all members of the European Union heavily regulate the credit-reporting industry using guidelines that, ironically, are based on principles drafted largely by the United States in the late '70s but never adopted here.

But while a certain amount of regulation is sensible—requiring credit-reporting companies to send credit reports to all their customers every year would be a good start—it might not be the best way to fix the problem. As the last five years have shown, on issues ranging from the environment to pharmaceuticals, regulations are only as strong as the regulatory impulses of the administration charged with enforcing them. The institutions to blame for identity theft aren't currently the ones who pay the bulk of the price. To fix that inequity, we need to shift the cost from the victim to those who can actually do something about it.

There is a successful precedent for this type of approach. In 1968, Congress passed the Truth in Lending Act, which imposed a variety of regulations on the lending industry. One notably simple provision was that consumers could be held liable for no more than $50 if their credit cards were stolen and used without their authorization. For anything above that, it was the credit-card issuer who had to pay. The result was predictable: Credit-card companies have since taken it upon themselves to develop a wide range of effective anti-fraud programs. Congress didn't tell them to do it, or even how. It just made them responsible for the losses, and the card issuers did the rest themselves.

The same method should be used for identity theft. There's no need to create mountains of regulations, which are uniformly despised by the credit industry. Instead, simply make the industry itself—and any institution that handles personal data—liable for the losses in both time and money currently borne by consumers. The responsible parties will do the rest themselves.

How would this work? Congress could assign specific minimum values—statutory damages—for each of the acts associated with identity theft. Extending credit without conducting adequate background checks, or issuing a faulty credit report thanks to undiscovered theft of identity, might be worth $10,000 per incident. Losing someone's personal information in the first place might be worth less—perhaps around $1,000—since only a small percentage of cases of information loss ultimately lead to a full-fledged theft of identity.

The establishment of statutory damages would allow consumers to bring personal or class-action lawsuits for any of these transgressions. (Currently, such suits are difficult to win because breaches of privacy are extremely hard to value—some courts even flirt with the notion that privacy has no value at all.) And consumers would not need to show that those responsible for the theft acted negligently. When your money is stolen from a bank, the bank is liable no matter how diligently it tried to protect it. That's why banks take care of your deposits. If the credit industry and other data-handlers knew that the legal system would hold them responsible for extending credit to impostors, issuing inaccurate credit reports, or losing data, you can bet they'd figure out better ways to stop those things from happening.

The beauty of this solution is that by giving the credit industry a financial stake in solving the problem, it uses market-based self-interest rather than top-down federal mandates. Instead of relying on a regulatory agency to levy fines—or not levy them, depending on the administration—it gives companies an incentive to change their behavior. Under this plan, credit agencies would no longer charge consumers for "credit protection" services. Rather, they would beg consumers to make use of them, free of charge and with maximum ease of access. Credit issuers and other businesses that offer credit would quickly stop opening up new accounts

without adequate background checks. And companies that handle personal data would finally get serious about implementing effective safeguards.

On a more basic level, the plan relocates the burden of responsibility for identity theft in a way that makes intuitive sense. If a company makes a mistake—by neglecting to conduct adequate background checks before extending credit, by issuing inaccurate credit reports or by failing to safeguard sensitive information—that company pays the price. It shifts power from corporations to individuals, based on a simple principle: Regular people should not have to go out of their way to protect themselves and their financial identities.

Identity crisis

Perhaps the chief objection to this approach comes from those who believe that Americans are already too quick to turn to tort-based remedies. We're all familiar with the crude caricature—painted by the business community and their allies in the Republican Party—of class-action lawyers as greedy and unscrupulous shakedown artists. But there are also serious economists who argue against torts on the grounds that they are intrinsically less predictable than regulatory solutions, since businesses can never be entirely sure what the law allows and what it doesn't until a jury decides a case. As Walter Olson of the Manhattan Institute puts it, "It's like saying, instead of writing a regulation, we'll tuck it away in an envelope and open it five years from now."

But in the case of ID theft, this might actually be a virtue. Michael Froomkin, a law professor at the University of Miami, points out that technology regulation is inherently problematic because innovations develop too quickly for Congress and the regulatory bureaucracies to keep up with. Identity theft is a new and rapidly-changing problem, one in which the details of responsibility vary greatly from case to case. There are benefits, therefore, to an approach that allows us to leave the specifics to be weighed separately in each instance, rather than relying on a one-size-fits-all regulatory solution.

Another objection to the tort approach is that many ID-theft victims don't know where the theft occurred, or have had their information stolen from their own wallets or trash cans—making it impossible to bring a lawsuit against the institution responsible for losing it. These victims, however, would still have entities to hold responsible: The banks or credit-card issuers that improperly offered credit to the thieves, and the reporting agencies that unfairly downgraded their credit. And victims who do know where their ID was stolen from would have an even wider range of targets. Indeed, consider what would have happened if this solution had been in place earlier this year when ChoicePoint was forced to admit that it had lost records containing personal information on 145,000 people. Under current rules, they have paid little price outside of some public embarrassment. But at $1,000 a pop, they would have been liable for $145 million—and a business-friendly attorney general wouldn't be able to help them out by lowering the fine or deciding not to pursue the case. It's a good bet that the episode would have motivated ChoicePoint—and just about every other company that handles large amounts of personal data—to keep that information safe next time.

Class-action suits are an inherently democratic remedy, putting enforcement power in the hands of consumers and their advocates instead of the government. They also put money in victims' pockets. In a recent study, law professors Theodore Eisenberg of Cornell and Geoffrey Miller of NYU found that, contrary to conventional wisdom, attorney's fees in class action suits average only about 20 percent—even less in large cases. Fully 80 percent of the damages go directly to consumers.

Indeed, the plan's ability to put consumers in control is one of its chief benefits. Framed as a way of increasing the power of ordinary Americans at the expense of large corporations and the federal government, it could be a political winner. And since Republican fealty—both ideological and financial—to the business lobby will likely prevent the party from uniting behind the idea, it could even help Democrats with one of their most urgent tasks: addressing the financial concerns of ordinary Americans. ◆