interview: mari frank

What your particular experience with identity theft? How did it happen?

In 1996 she was a victim of "identity theft" when a woman assumed her identity and rang up over $50,000 in credit card debt. Frank wrote a book, From Victim to Victor, on what she learned about how to protect against identity theft. She also **publishes a web site** with further resources for protecting privacy.

I was a victim of identity theft in 1996. I got a phone call from a bank that I'd never heard of and they said, "Is this Mari Frank?" And I said, "Yes." And the woman said, "This is the Bank of New York in Delaware, and we want to know why you haven't paid your $11,000 bill to us." And I said, "I'm sorry, I'm running out now. You have the wrong name, the wrong number. I don't know who you are. I've got to go." And the woman said, "Wait a minute, is this your Social Security number and your birth date?" And of course, by then, I started to get worried, and I said, "What are you looking at?" She said, "I'm looking at the billing statements that we have for you and your credit report. And I said, "Where did you send those billing statements, where did you send that credit card?" She gave me an address four hours from my home that I'd never heard of. And I said, "I've never lived there."

And so then I knew right away that it was fraud, and I asked her what else was on the credit report. Obviously, she wouldn't tell me. I ordered my credit reports. I found that over $50,000 worth of credit was stolen in my name. Some woman had purchased a red convertible Mustang in my name as well. She had driven down to my law office, stolen my business cards, was parading around as an attorney in my name. She had rented a car. She had gotten a fake driver's license with her picture and my name. She had gotten credit cards so she could rent a car, and totaled it, and I was being sued by Thrifty Rental Car.

So it took me over 500 hours to clean up the mess. I started clocking it after about two weeks--that's the attorney in me. It took me about 11 months to clean up the mess. Now, I did this myself, and I knew what I was doing because I'm an attorney. I'm not very shy. I'm able to write letters-- I do it for a living. And it was overwhelming for me. I've spoken to victims. Sometimes they've been victimized for 14 years. It can take hundreds of hours and thousands of dollars to clear it up. It's a total nightmare for them.

Was the person who "stole" you an educated person? Was she computer literate?

No. . . . I was very fortunate, by the way. In only about 10% of the cases does the victim ever even find the imposter. I was very lucky, and that's because I worked very hard to find it. The law enforcement agency that helped me only helped me because the watch commander himself was a victim. So that's why I was very lucky, and people shouldn't think that they're going to get the kind of help that I got. I was fortunate.

The person who stole my identity . . . was really a secretary and she was working in a law office. And she had access to the computers and the internet. And because the law firm had a subscription with a re-seller of credit reports, she could go online and order several different credit reports. She could just pull up names, and that's what she was doing. So she was actually assuming quite a few identities besides mine. I never saw her until I saw her on television. I saw her mug shot. I never knew her. She did plead guilty to six counts of a felony credit card fraud, because we didn't have an identity theft statute at the time. She did a two-month work furlough program for her punishment, still driving the red convertible Mustang.

"you can minimize risk by keeping your confidential information as confidential as possible. But the reality is, **if someone wants to get your information, all they have to do is go online.**"

And nobody paid for that car.

Right. And interestingly enough, after that I was incensed by how the system didn't work. I was actually more incensed with the credit card companies and the credit reporting agencies for their negligence than for this woman. She was 36 years old, she was a single mom, she was a methamphetamine addict. I got to the point where I almost felt sorry for her because she had to do this. I never knew her and I wasn't real happy with her, but basically I felt that the companies did nothing to protect me. Nothing. They didn't verify identity. They didn't authenticate. They just issued credit like it was candy, and then after the new address was reported to the credit reporting agencies, she got pre-approved offers sent to her like candy to her door. So I really felt like the whole financial industry was facilitating the crime.

And law enforcement at the time had no teeth to help me, because there was no identity theft statute. So I worked in California to help get two laws passed to make identity theft a crime. I went to Washington. We now have a federal crime law that makes identity theft a federal felony, with up to 15 years in prison. Now there are about 40 states with identity theft statutes, and there was only one when I was a victim. So from 1996 to the year 2000, quite a bit has happened. . . .

How widespread is identity theft?

Identity theft has become an epidemic. In the United States, we know that there were over 700,000 victims last year. And that's just a very modest calculation, based on the fact that one of the three credit reporting agencies received 62,000 calls a month. Now it's starting to happen in other countries as well, because we get calls from Japan, from England, from France and from Canada. . . .

I get the impression that most of this is one-shot theft and abuse of somebody else's credit card.

No, this is not just one-shot abuse. That is one form of identity theft. . . . . [But] you can pay to get someone's Social Security number on dozens of information broker sites. Then you're talking about complete identity takeover. When somebody gets your Social Security number-- at least in the United States--that's what they're going to use, because that's the key identifier in identity theft. They get that Social Security number, and from that, they can apply for credit cards and credit lines. They establish a whole new profile, and it goes to an address that's other than yours.

So you have no idea that this is happening, maybe for years, because all of this credit is going to another address. Meanwhile, your credit profile, maybe your American Express or your Visa, is coming to your home. There's no fraud on it--nothing. Everything looks perfect, so you have no idea until something happens, like you get a fateful call from a company that says, "Why haven't you paid your bill to us?" Or you apply for credit to buy a new car or a new house, and they say that your credit is ruined. And you look at your credit report and you see fraud on there that you never knew existed. . . .

Now in the olden days, you really have to actually go to maybe get court records or do some other things to commit identity theft. That would take much longer. So, yes, there was identity theft. And there were people who were able to do that as a profession, people who were very smart about getting your information--people like private investigators, information brokers. Now they put that online. There are hundreds and hundreds of sites that you can go to. You don't have to spend a great deal of money or a great deal of time. It's transferred to you in just a second.

Surely somebody is doing something about this. Surely people in authority recognize the perils here.

Well, people are starting to recognize this, because we're bringing this to the forefront. There are two bills pending in the United States Congress right now. One is called the Identity Theft Protection Act of 2000, and the other one is the Social Security Protection Act of 2000. The Social Security Act of 2000 says that you cannot sell a Social Security number anywhere for money-- that it would be illegal to do so.

The Identity Theft Protection Act also addresses some of the issues about the credit reporting agencies and the credit card companies, who have been so lax in verifying and authenticating identity. For example, when a creditor gets an application with my name and it's an address that's not on my profile, if this bill passes, they would have to verify it before they could issue credit. So there would actually be sanctions for a company who issued a credit card to a fraudulent address without checking.

So, yes, we are starting. . . . The problem is, if you have laws in the United Sates and you don't have the same laws in other countries, we've got all this conflict of laws, because the internet is global.

What's the worst case that you've heard of?

Online, the worst case was actually a call I got just last week from a woman. She was desperately crying that her ex-husband's girlfriend had opened up an email account in her name and had gone online to send emails to the husband pretending to be the wife, threatening to kill their child, threatening to kill herself, making all sorts of allegations about things that were going on. So when he goes to court next week, he can say that she was an unfit mother and . . .

. . . And psychotic.

. . . and psychotic. Then she cannot get custody. And so this woman found out that the email account actually had been opened from a university where this man's girlfriend is going to school. She had to pull in a computer expert to try and help her in her family law case. And I don't know what's going to happen yet. She called me, and I told her things to do. But this is such a new field, and people are looking at her like she's crazy. She lives in a little town in the Midwest where people have no idea about this stuff. And the problem is that the technology is there, but the safeguards are not. . . .

Assuming that there will never be sufficient public controls or communal control to prevent the abuse, what does the individual do?

The individual can do certain things to **minimize their risk**, but I have to tell you, there's nothing that you can do to guarantee it. There are certain things you can do that involve just being more aware. For example, getting your credit report and looking at it at least twice a year, and seeing if there's any fraud on it. That is the first thing to do--make sure that you get it quarterly and see what's on there.

Because we're finding out that there's so much criminal identity theft, now I'm telling people go and do a criminal background search on themselves at least once a year. Find out if someone has a murder arrest in your name. That happened to one of my clients last year. He had no idea for two years that there was a murder arrest, and he couldn't get a job.

He was officially a convicted murderer?

He wasn't a convicted murderer. He was supposedly arrested for murder. When his Social Security number was mixed with another Social Security number, the name was wrong. But when he applied for jobs, he kept getting denied employment, because it was coming up that he had been arrested for murder. I'm still dealing with that case right now.

But I'm telling people to get your background searched and see if someone is committing a crime in your name. I get probably a dozen calls a month just from criminal identity theft and maybe a hundred calls a month on financial identity theft.

So the first thing you can do is to get your credit report. The second thing is to shred all your information that you have offline. For example, if you get a bank statement and it's got your Social Security number, shred it. Don't keep any information around, because people can go and do what we call "dumpster diving." They go through your trash and they fish out what they want.

They can do it at work. Be careful at work. Does your badge have your Social Security number on it? In other words, make sure that you limit the use of your Social Security number. Don't carry it around with you. Don't give out personal information online. . . .

And another thing we tell people to do is to even shred information that's on your computer. Confidential information should be encrypted, and any information that you want to get off your computer, you have to shred, because if you delete it, it does not just delete.

Another thing you should do is make sure that you don't give confidential information by cell phone, or by a remote phone, or on the internet unless it's encrypted. Put up firewalls so someone can't come in and steal your information from your computer.

But why should the burden be on us, as citizens, just to protect our own identity? . . . We have to opt out of all of these companies that are selling our information. We have to spend a fortune to find out who's stealing our information. It really just seems that it is a tremendous burden on the citizens of our country. . . .

What was the result of your miserable experience?

I created the Identity Theft Survival Kit, because it's the kit I wish I'd had when it happened to me. In it, I've got tapes with experts from across the country, including the Secret Service. I've got a book that's got step-by-step instructions on how to stop being a victim. And I've got all the legal letters that you need to write so you don't have to hire an attorney. And the good

news is this whole thing is tax-deductible, under the US tax code for fraud losses.

The Identity Theft Survival Kit and Frank's book are available for purchase on her web site, **Identitytheft.org**

home · **who are hackers?** · **risks of the internet** · **who's responsible** · **how to be vigilant** · **interviews**
discussion · **video excerpts** · **synopsis** · **press** · **tapes** · **credits**
FRONTLINE · **wgbh** · **pbs online**