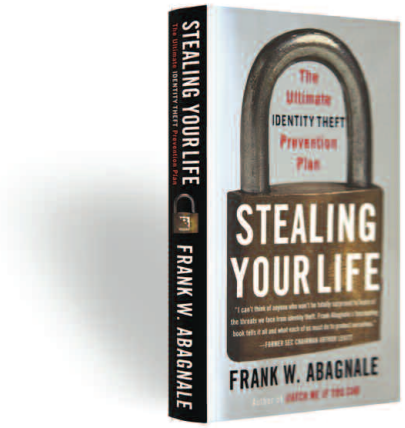
SOUNDVIEW Executive Book Summaries®

FILE: PERSONAL



by Frank W. Abagnale

CONTENTS

The Sweetest Con of All
Page 2

The Next Victim — And It's You
Pages 2, 3

The Road to Becoming You
Pages 3, 4

It Could Be Public Enemy No. 1 or It Could Be Grandma
Page 4

What Your Duplicate Is Doing As You
Page 4

The 20 Steps to Prevent Identity Theft
Pages 4, 5, 6

Remember That Privacy Statement You Threw Away?
Pages 6, 7

The Crime That Keeps on Stealing
Pages 7, 8

Staying Two Steps Ahead (Or Three)
Page 8

The Ultimate Identity Theft Prevention Plan

STEALING YOUR LIFE

THE SUMMARY IN BRIEF

Before the age of 19, Frank Abagnale had successfully conned millions of dollars worth of checks while posing as a Pan Am pilot, doctor and legal prosecutor. It is his early life that has been captured in his best-selling memoir and 2002 blockbuster film *Catch Me If You Can*. However, now he has gone from fraud to a fraud-fighting consultant.

When Abagnale trains law enforcement officers around the country about identity theft, he asks them for their names and addresses and nothing more. In a matter of hours, he can obtain everything he would need to steal their lives: Social Security numbers, dates of birth, current salaries, checking account numbers, the names of everyone in their families and more. This exercise illustrates how easy it is for anyone from anywhere in the world to assume your identity and, in a matter of hours, devastate your life.

Considering that a fresh victim is hit every four seconds, this summary offers important tips and techniques from an unsurpassed authority on the latest identity theft schemes.

Abagnale offers dozens of concrete steps to transform anyone from an easy mark into a hard case that criminals are likely to bypass. Several anecdotes of creative criminality are included, which are as entertaining as they are enlightening. This summary provides clear, practical ways to protect yourself from one of today's most common crimes.

IN THIS SUMMARY, YOU WILL LEARN:

- Who is at risk for identity theft.
- Why you should avoid offers that appeal to greed or fear in exchange for personal data.
- How to monitor your credit report regularly and know if anyone's been "knocking on your door."
- How to identify the people stealing identities.
- Why you should read privacy statements carefully and choose to opt out of sharing information whenever possible.

Published by Soundview Executive Book Summaries, P.O. Box 1053, Concordville, PA 19331 USA

by Frank W. Abagnale

The Sweetest Con of All

Identity theft is the wholesale lifting of someone's identity for illicit gain. It's stealing that identity, then using it to access a person's bank account, their personal information and their personal finances. It's becoming someone else for the bucks.

The rewards are enormous for a thief. Identity theft will afford you access not only to someone's wallet and bank account but to his or her very life, character and ability to borrow and spend. Technology has made identity theft easy to execute behind the shadowy cloak of a computer keyboard. You don't even have to be in the same city or country as your victim. You can steal someone's identity without being able to speak his language or pronounce her name.

A Federal Crime

The federal Identity Theft and Assumption Deterrence Act, passed in 1998, made identity theft a federal crime. It carries maximum penalties of 15 years in prison and substantial fines. But police say they have little incentive to go out and arrest an identity thief. The FBI is under a directive not to investigate any white-collar crime under $100,000 in value, due to lack of resources and the shift in manpower over to fighting terrorism.

Who's at Risk?

In recent years, identity theft has become a crime so versatile that the list of potential targets is endless. Anyone who has a credit card or a bank account, or who pays bills is at risk. Anyone who has a mortgage, a car loan, a debit card, a driver's license, a Social Security number, phone service, health insurance or a job is also at risk. If you use the Internet, you are at risk.

A 35-year-old New York busboy had the hubris to choose names off the Forbes 400 list, including Ross Perot, Oprah Winfrey, Michael Bloomberg and Ted Turner, gleaned additional information on them from the Internet, and became them. Tiger Woods was victimized by a California man who rented a moving truck and a storage locker in his name. Even the dead can become targets of this insidious crime. Identity theft is the fastest growing criminal activity in the country.

Every Four Seconds

In 2001, there were about 750,000 documented victims of identity theft, and losses to banks and credit card companies amounted to $5 billion. In 2003, the Federal Trade Commission released the most exhaustive government study to date on identity theft, estimating that there had been 27.3 million victims in the prior five years. In 2004 alone, around 10 million consumers suffered from some variation of identity theft, and losses exceeded $54 billion. In 2005, it's believed that an identity was stolen *every four seconds*.

By shining a light on the diabolically creative and clever criminal mind, you as a consumer can clearly understand just how vulnerable you are to somebody becoming you. To effectively keep this crime from happening to you, you need to understand how it works in a comprehensive way — what the telltale signs are, who does it, how thieves get information and what they do with it. ■

The Next Victim — and It's You

A woman with especially fussy tastes had been searching for her dream house for what seemed like forever. And then there it was: a postmodern house that was just the right size, in just the right neighborhood, and best of all, at just the right price. She had to move fast — others

(continued on page 3)

The author: Frank W. Abagnale is the author of the best-selling memoir *Catch Me If You Can* and *The Art of the Steal*. He works closely with the FBI and corporations around the world as an expert on counterfeiting and secure documents.

For additional information on the author, go to: http://my.summary.com

Published by Soundview Executive Book Summaries (ISSN 0747-2196), P.O. Box 1053, Concordville, PA 19331 USA, a division of Concentrated Knowledge Corp. Published monthly. Subscriptions: $209 per year in the United States, Canada and Mexico, and $295 to all other countries. Periodicals postage paid at Concordville, Pa., and additional offices.

Postmaster: Send address changes to Soundview, P.O. Box 1053, Concordville, PA 19331.

Available formats: Summaries are available in print, audio and electronic formats. To subscribe, call us at 1-800-SUMMARY (610-558-9495 outside the United States and Canada), or order on the Internet at www.summary.com. Multiple-subscription discounts and corporate site licenses are also available.

Soundview
Executive Book Summaries®

CHRIS LAUER – CONTRIBUTING EDITOR
ATHENA NICOLAIDES – GRAPHIC DESIGNER
MELISSA WARD – MANAGING EDITOR
SARAH T. DAYTON – EDITOR IN CHIEF
REBECCA S. CLEMENT – PUBLISHER

The Next Victim — and It's You

(continued from page 2)

had appointments to view it that afternoon — and so she said she'd take it. All that was left was to fill out the necessary paperwork, talk to the right people and have the bank process her loan application. Then word came back from the bank, and its verdict was bad. The mortgage was denied. Her credit was insufficient, and there was nothing they could do about it. She was shocked.

What Went Wrong?

The deal breaker was identity theft. While she had been minding her own business and paying her bills on time, an impersonator posing as her was making mincemeat of her credit. Her doctor's receptionist had pilfered her information from his files, obtained multiple credit cards in her name, and then run them up to their limits, costing the woman the house she so fervently desired.

There are four key events that suggest that someone has become a victim of identity theft:

1. Denial. Denial of credit is the first sign of identity theft. Another form of denial is a notification of a rate increase on your car insurance or home insurance, or that your insurance is being canceled.

2. Ripped off. It's a pretty good tip-off that something is wrong when your credit card, bank or other financial statement contains charges that you never made. An even more obvious tip-off is a statement for a credit card or loan that you didn't know you had.

3. Harassed and hounded. When you get calls to collect on debts that you never incurred, an alarm ought to go off in your head. Get the information from the collector, then contact the company. When you speak to the company, tell them that you didn't purchase anything from them or apply for a loan, and if they'd like a sworn affidavit, tell them you'll send it.

4. Where did the mail go? If your bills stop coming, or there's an unusual decline in the quantity of mail you receive, that's a problem well worth investigating. It might mean that an identity thief has stolen your mail or has changed the address on your credit card statement so you won't notice the fraudulent charges on your account.

Often there is no sign at all that you've become the target of identity theft. Complacency always works to the very profitable benefit of criminals. ■

The Road to Becoming You

The Internet is one of the most versatile research tools a criminal has ever been handed. It's no exaggeration to say that there are thousands of free and paid resources on the Web that can be unsuspectingly used for identity theft.

Every time you share a piece of information about yourself, without obtaining a binding guarantee that it will not be sold or shared, that information instantly enters the public domain and becomes fodder for an expanding information industry. The only exception is medical information. For that to be shared, a release has to be signed.

Between nosy washer warranties, dog pound questionnaires and computer disks tumbling off trucks, your private information is vulnerable in a million different ways, limited only by the ingenuity of the thieves.

Nigerian Letter Scams

You might have received an e-mail that purportedly comes from the wife of a Lebanese businessman who has been killed in an explosion in Beirut. He left behind $86 million, and $20 million of it is yours if you help get the money into the United States.

This is one version of a classic scam with very long legs. This type of trap is known as a Nigerian Letter scam or a 419 letter, named after the pertinent African criminal code under which it can be prosecuted.

As identity theft has become the top game in town, Nigerian Letter scams have been reconfigured to steal your identity information. They don't necessarily even ask for your bank account number anymore. They'd rather get your name and Social Security number and use them for a full-scale identity assumption.

Phishing

These e-mails, and numerous other renditions, are called phishing attacks. Today, phishing is one of the most productive ways identity thieves gather their source material. Phishing is highly efficient. Sending spam e-mail out to a million people doesn't cost a cent, but every

(continued on page 4)

Fake Bank Ads

One popular e-mail phishing category is fake bank ads. If you call, you are asked the usual personal information. Later on, customers are told that they need to make an advance payment on their loan through a Western Union wire transfer to an address in Canada, identified as a "third-party consultant."

If you follow the instructions, the criminals succeed in making a double strike: They acquire some immediate cash, plus they get sufficient personal information to launch an even more rewarding identity theft.

The Road to Becoming You

(continued from page 3)

"phish" that is hooked can be worth thousands of dollars.

The standard strategy is to phish using a cover that people are likely to recognize and trust, usually a bank, brokerage house, corporation or government agency. Citibank, eBay and AOL have been common choices. The message will set forth a phony but believable reason why you need to respond with your personal information.You're asked to respond to the e-mail or click on a linked Web address and answer the questions there. ■

It Could Be Public Enemy No. 1 or It Could Be Grandma

An astonishingly diverse group of individuals is perfectly comfortable making at least a part-time living as identity thieves. They are people of all ages, all races, both sexes, all cultures, all religions, educated and uneducated, blue collar and white collar.

According to a 2004 study by Judith Collins, a professor at Michigan State University, in more than a thousand randomly selected identity theft cases, roughly half the culprits were women.

It's the Woman Who Served Your Omelet

A 23-year-old waitress at a popular restaurant in Fenwick Island, Del., was arrested for using a hand-held credit card reader, known as a skimmer, to steal identities. The device reads and records the information on magnetic stripes, thus allowing criminals to make fake cards. She explained that at a party, a Russian man, who set up the scheme, approached her. He paid her $10 for Visa and MasterCard numbers and $15 for American Express.

Collins and her students at Michigan State, in their examination of identity theft complaints that had been filed with the police, called or wrote these victims and asked them, "How did the person get the information to steal your identity?" Of those who knew, a shocking 70 percent responded that the thief obtained the information from a low-level employee who sold it to somebody else.

Your information is everywhere, and workers with little if any security clearance know where the stuff is — and have the means and authority to get to it. ■

What Your Duplicate Is Doing as You

In early 2003, a 72-year-old British man named Derek Bond, a retired engineer, grandfather of six, Rotarian and wine enthusiast, was arrested in South Africa, where he had been on a wine-tasting vacation with his wife. Told that the FBI had identified him as a wanted fugitive, he was imprisoned in a Durban jail. He was fingered, the authorities informed him, for masterminding a marketing scheme supposedly intended to market telephone calling cards that fleeced more than 200 investors of millions of dollars. Though he insistently professed his innocence, the police were convinced that they had their man. For three weeks, Bond was forced to sleep on a concrete floor.

After 20 days, he caught a break. The real culprit, an identity thief, was nabbed in a Las Vegas hotel room. Bond was released. It turned out that the crook had been using Bond's identity since as far back as 1989. Oddly enough, they were the same age.

They Go Bankrupt

Crooks aren't particularly proficient at managing their finances, and being freelancers, their incomes can fluctuate a lot. Once they start relying on your credit, they draw you into all sorts of nasty outcomes.

Not long ago, a woman saw a notice in the mail that was addressed to her son. She opened it and was stunned to find him being summoned to appear at a meeting of creditors that was to be conducted as part of his Chapter 13 bankruptcy case. This was rather disturbing. Her son wasn't in any debt that she was aware of. After all, he was 5 years old.

A sweeping new federal bankruptcy law went into effect in October 2005, designed to eliminate so-called "bankruptcies of convenience" by people who have abused their credit without ever intending to pay the bills. The law is having a perverse effect on victims of identity theft. Debtors now have to repay some of their old debt, and there are no exclusions. That means that if an identity thief runs up excessive debt in your name and files for bankruptcy, you'll be held responsible for the bills. ■

The 20 Steps to Prevent Identity Theft

Identity thieves — the professionals, at least — spend all their time trying to outwit you so they can steal your money, while you spend at most a small portion of your time trying to keep them from getting it. So the odds distinctly favor them. But you can reduce those percentages significantly if you take a number of fairly simple precautions.

The following are the 20 crucial steps that can best

(continued on page 5)

The 20 Steps to Prevent Identity Theft

(continued from page 4)

keep you from becoming a victim:

1. Check your credit report. Keeping abreast of your credit history is your best self-protection technique by far. If an identity thief uses your Social Security number and name to open a new credit card account with a fake address and phone number, you may not find out about it until the damage is long done — unless you check your credit report periodically.

2. Don't give out your SSN. Just because a form contains a space for your Social Security number doesn't mean you have to fill it in. A good rule to adhere to is, the less information you give out, the better.

3. Protect your computer. If you're using a wireless connection to access the Internet, make sure it's secure. Use an encrypted service. It's vital to update your virus protection regularly. Install an adequate firewall. Assume that any e-mail that asks for your personal information is a fraud.

4. Keep track of your billing cycles. A missing bill doesn't mean that a credit card company or a mortgage holder is giving you a month off. Rather, it may mean that a thief has changed your address. If you know the MasterCard bill usually comes on the 15th and now it's the 27th, then something's up. Call and figure it out.

5. Examine your financial statements like an obsessed accountant. As soon as a credit card statement arrives, go over it carefully to make sure you really bought all that stuff. If you didn't, deal with it right away.

6. Guard your mail from theft. Make a practice of picking up your mail as soon as possible after it is delivered, lest some well-intentioned thief concludes you won't mind if he takes it. Consider investing in a locked mailbox, or if you live in a high-crime area, play it extra safe with a post office box. Take your outgoing mail to a drop box rather than leaving it in the mailbox in front of your home.

7. Invest in a shredder. Get into the habit of shredding all documents before you toss them in the garbage. This goes for all bills and papers that contain personal information, especially Social Security numbers and financial account numbers. And it certainly goes for those pre-approved credit card and loan offerings. If you're going to sell or discard your computer, wipe the hard drive.

8. Practice safe shopping. Shop only from secure sites that will encrypt your order information and your credit card number before sending them to a merchant.

9. Avoid sketchy ATMs. Be skeptical of portable machines that you see in delis and hotel lobbies, especially ones that have a cord protruding from the back that's not plugged in. That means the data isn't being sent anywhere — it's just recorded for a crook's eyes. Stick with real, secure bank ATMs.

10. Be suspicious of unexpected calls or letters. When a business calls or e-mails you and asks for personal information, indulge in a little healthy paranoia. It's usually a clue that something's wrong. Make it a rigid policy not to get personal unless you're the one who initiated the contact.

11. Put real passwords on your accounts. Come up with one password that you can use in multiple applications that no one else will know. And never write it down. A strong password is a random eight-character combination of numbers, letters and symbols. Better yet, pick something familiar to you but that only you will know.

12. Keep your credit card close when shopping or eating out. When you're out spending money, watch how salespeople and waiters handle your cards — make sure they don't have a chance to copy them. Be especially alert at a store or restaurant that you've never been to before.

13. Use safe checks, and use them sparingly. Make it a habit to always get your checks from your bank, because banks are far more likely to use ones that contain fraud protection features. These include things like a watermark, thermochromatic ink, chemically reactive paper, and light-sensitive ink and fibers.

14. Secure the home front and office front. Find a non-obvious location in your home where you can store your Social Security card, passport and all records, including credit card statements and tax forms, which contain personal information. Don't leave valuable personal information on your desk or computer screen.

15. Carry only what you need. Leave your Social Security card at home in a secure place. Carry only credit cards you plan to use.

16. Spring clean your credit cards. If you aren't regularly using a credit card, cancel it. The more cards you have, the more opportunities a thief has to steal from you. Maintain organized records of all your credit cards so that if a theft does occur, you can report it promptly and thoroughly.

17. Opt out. Get your name off of marketing lists that get sold and resold. If fewer businesses have and sell your data, fewer thieves will be able to steal it.

18. Read privacy policies. They are essential for understanding what your bank, financial institutions and

(continued on page 6)

The 20 Steps to Prevent Identity Theft

(continued from page 5)

other businesses that you deal with do with your information. They will also tell you what restrictions you can place on the dispersal of your information. Elect all the restrictions available to you.

19. Protect a deceased relative. When someone dies, contact the credit bureaus and have a "deceased" alert put on the person's reports. Inform Social Security of the death yourself, directly, with a copy of the death certificate.

20. Place fraud alerts on your credit reports. Putting a *fraud alert* tag on your credit report will limit a thief's ability to open accounts in your name. If you've been a victim of identity theft, you can place an extended fraud alert on your report that remains in place for seven years. These alerts will slow down your ability to get credit, but as long as you're willing to accept that slight inconvenience, give yourself all the protection that's available.

Nothing is foolproof. But if you make it hard for thieves to get your identity, then their inclination will be to leave you alone and try someone else. ■

Understanding Trade Lines and the Meaning of R2

One of the primary reasons identity thieves are so successful is that most people don't bother to read their credit report or even know how to read one. And even those who do often fail to appreciate how important it is and how a single line buried somewhere in the dense body of their report can radically affect their future.

As it is, something like 4.5 billion pieces of data are entered each month into credit records: bill payments, bankruptcies, court judgments, overdue child support payments, foreclosures and liens. One reason to read your reports religiously is that much of that information is wrong.

The Credit History section of your credit report enumerates all of your credit accounts and credit behavior. It's basically your history of borrowing, reduced to names and digits.

The accounts enumerated here are known as *trade lines*. Each trade line includes the creditor's name and the account number. Each trade line discloses when you opened the account and the nature of the credit.

When you look over your report, check each trade line very closely for accounts that you don't recognize. For the accounts that are legitimately yours, make sure the number in the Balance Owing column jibes with what you've actually spent.

You Can Correct Your Credit Report

Any time you detect something amiss in your credit report, correct the discrepancy as quickly as possible.

The first thing to know is, it's your right to have your report corrected. The law states that both the credit bureaus and the information sources — the credit grantors who gave them the information about you — are responsible for correcting inaccuracies in your report. To make sure they really do, attack on both fronts: contact the credit bureaus as well as the information providers. Call all three major credit bureaus — Equifax, Experian and TransUnion — then follow up in writing. The credit bureau is allowed 30 days to investigate your case. The credit bureau then sends you a written report on the outcome.

Payment Codes

Often the reports rely on payment codes that range from 1 to 9. The reports will use "R" to stand for revolving credit and "I" for installment, and then grade each account.

An R1 or I1 means you pay that bill within one month — in other words, on time. R2 means you pay within two months, and so on into escalating lengths of tardiness. R7 or I7 means your debts have been bunched together and are being repaid under consolidation. R8 is rather dismal news — your debt was satisfied by repossession. The worst news is an R9, which is when you've defaulted and the debt has been deemed uncollectible. R0 means you've just entered the wonderful world of credit and haven't been out there long enough for the credit wizards to judge your behavior.

If a trade line is unfamiliar to you but the bill payments are up to date, don't ignore it. An identity thief may have used your name and ID to get a loan, which he or she is temporarily repaying promptly so as not to attract attention. Don't make the mistake of thinking that an up-to-date account is a benefit to your credit score. You could wind up being denied credit later on when the person suddenly defaults on "your" loan — or even simply because you now have too much credit. ■

Remember That Privacy Statement You Threw Away?

A privacy policy essentially tells you what personal information a business collects and how it collects it. It tells you

(continued on page 7)

Remember That Privacy Statement You Threw Away?

(continued from page 6)

how the business uses your information, who it shares it with, and what "opt-out" options you have for limiting how your personal information is compiled and distributed.

When it comes to the opt-out options contained in privacy policies, there's only one smart move to make. Use them, all of them.

Selective Shopping

Read your privacy statements and then evaluate the contents to decide who you want to do business with. Select your banks based on who does a better job of protecting your information.

If your bank doesn't offer the controls that it ought to, use another one. If a shopping site falls short in its privacy policy, shop at another place. Or complain vigorously about the policy, and maybe a miracle will happen and they'll rectify the deficiencies. ■

For additional information on privacy policy statements, go to: http://my.summary.com

A Farewell to Checks

These days, Americans write something like 39 billion checks a year. That figure is starting to come down a little bit, but the prevalence of checks is still huge.

Writing checks is just too dangerous. Every check you write to the hairstylist or the cleaner has your name and signature, your bank's name and address, your account number and your routing number. Salespeople routinely ask for a driver's license or work number, as well as other personal information, and scribble that on the check. Certainly just the check front alone contains more than enough information to draft on your bank account — or become you.

Washing Checks

If you are going to write a check to pay the electric bill or the gas bill, don't put it in the mailbox outside your house. Typically people put their outgoing mail in the mailbox and put the flag up, which is sort of like raising a red flag. It makes you vulnerable to an extremely common scam called *washing checks*.

There are criminals who drive through neighborhoods early in the morning to see that red flag, and remove the envelope containing your check to the electric company. They take that check home, put a piece of Scotch tape over your signature, and use an everyday household chemical to wash off all the information on that check except your signature. Then they can make the check out to themselves, fill in any amount and cash it.

So if you're going to mail a check, take it directly to the post office mailbox and mail it there. An even better precaution is to use a pen with permanent ink. ■

They Got Me — Now What?

No matter how many precautions you take, you might become the victim of identity theft. It's important to follow an orderly protocol. Here are the steps to take:

1. **Call the credit bureau fraud departments.** Report the crime to the three credit bureaus so that they can put an alert on your file.

2. Shut down all compromised accounts and documents. Immediately pull the plug on the old and the new, both your own accounts that the thief may have been misusing and any new accounts that he or she opened in your name. When you reopen your accounts, make sure you have a new account number, and guard it with a fresh password.

3. File a police report. The report will help you remove the fraud from your credit report. Companies will want some kind of proof that you really are a victim. A police report is the best proof you can offer, because creditors assume you wouldn't file a police report unless you really meant it.

4. Establish good records — of everything! Send all letters certified mail, return receipt requested, from your local post office. That way you'll have a record of when you sent something and when it was received.

5. File a complaint with the FTC. Finally, once you've determined as best you can the extent of the fraud, file a complaint with the Federal Trade Commission, which can be done online at www.consumer.gov/idtheft, or by phone at 1-877-IDTHEFT. The FTC doesn't get involved in resolving individual cases, but the complaint is useful information in its work to investigate fraud, and it could spur a law enforcement response. ■

For additional information on credit bureau fraud departments, go to: http://my.summary.com

The Crime That Keeps on Stealing

The dark side of identity theft is that it doesn't necessarily end, even when you take the recommended steps.

(continued on page 8)

The Crime That Keeps on Stealing

(continued from page 7)

You're dealing with persistent criminals who don't relent and an imperfect resolution system. That combination makes it very hard to completely come out from under this insidious crime.

Even after one particular thief appears to be finished stealing your money, he or she continues to steal your sense of security. Once you've been violated, it's hard to feel safe again.

An elderly couple had a registered nurse living with them for years, caring for the man, who was sickly. When he died, the nurse left — along with his identity. When his widow wrote a check for his funeral, it bounced because the nurse had already cleaned out his account.

Criminal Records Live Forever

When thieves commit other crimes in your name, you really face a burden that won't go away. It's easy enough to check your credit record, but there's no easy way to check your criminal record. If an identity thief has put a blot on your record, you don't know it until the police stop you. And you never know when it's going to reappear. ■

Write Your Company and Congressperson — Now!

Society and public officials have a big responsibility. Congress and state legislatures need to provide consumers with more protection; so do the businesses that you patronize.

A group that calls itself Artists Against 419 — exasperated that law enforcement and companies don't do more about phishing scams — has actually been pursuing thieves on its own, a rare instance of a vigilante group aimed at white-collar crime. When one man found out that a department store had a videotape of the thief who had assumed his identity, he managed to obtain a copy of the tape and convinced a local TV station to run it on the evening news. Several viewers recognized the man and called in to finger him.

Every company in America, every government agency, every municipality and every health-care provider has to ask itself one simple question: What are we doing to protect the identity of our customers and our employees?

As a consumer, you've got to push them to get an answer to that question, because if they don't have the right answer, they're putting you at needless risk. ■

Staying Two Steps Ahead (Or Three)

Identity theft will intensify in its tried and tested forms and in new variations as well. Identity thieves have already begun to invade cell phones and personal digital assistants and steal data from them. We're going to continue to see information swiped on a massive scale from companies and databases and sold not only in this country but overseas to those who wish to assume the identities of Americans. Even terrorists would be able to slip into someone's identity and get a job here and join a sleeper cell, because it is so easy to do.

Every precautionary action we undertake to prevent identity theft, therefore, has to take into account what could come next. Crime is a full-time job for its practitioners. Every move to thwart it has to anticipate the criminals' next move.

Here's a good example: The average phishing site lasts only five days before the crooks abandon it and move on to a new one. Why? It usually takes about six days for law enforcement or security experts to shut it down. So the thieves head elsewhere just before they hear the footsteps of the authorities closing in.

So you have to think two (if not three) steps ahead.

Protect Yourself

We need to wake up to the fact that identity theft is a drama still in its first act. You must take steps to protect yourself. And you must start thinking like a criminal, and remember that a crook always looks for the easiest route to riches. Don't hand him or her a map.

We can't be idealistic and think we can stop identity theft altogether, but we can slow it down — a lot. We can possibly transform identity theft from a growth industry to one that is in steady decline. To do so, we must take prevention more seriously and press businesses, legislators and law enforcement to do the same.

We live busy lives, but this is a terrible problem. Remember, everyone is a potential victim. ■

Recommended Reading List

If you liked *Stealing Your Life*, you'll also like:

1. ***What Got You Here Won't Get You There*** **by Marshall Goldsmith with Mark Reiter.** The corporate world is full of intelligent and skilled executives, but few will ever reach the top and, according to Goldsmith, subtle nuances make the difference.
2. ***Wikinomics*** **by Don Tapscott and Anthony D. Williams.** The authors address how the Internet's social network offers new, decentralized ways to produce content, goods, services and profit in the emerging world of massive peer collaboration.
3. ***Words That Work*** **by Dr. Frank Luntz.** To effectively obtain the power of communication, you must learn that it's not always what you say, but how you say it. Luntz offers sound advice on how to tactically use words and phrases to get what you want in life.