The Motley Fool®

Master Your Money

SPECIAL REPORT — PART THREE

How to Protect Your Identity From Being Stolen and Your Credit From Being Wrecked

Is everyone out to get you? Sometimes it seems that way. As we were preparing this special free report — the third in our "Master Your Money Series" — yet another massive security breach made the front pages.

The victims? More than 26 million veterans.

The bounty? Data including Social Security numbers, dates of birth, and other sensitive information that could be used to steal the identities of the victims.

This wasn't a high-tech coup by a team of talented hackers. Nope, equipment containing the information was swiped from the home of a Department of Veterans Affairs employee in what was likely a random burglary. While the crooks probably did not know at the time that the computer's motherboard contained a mother lode of valuable data, the ensuing front-page publicity has no doubt given them a clue by now.

The Silent Sniper

Like a slow gas leak or the onset of a debilitating virus, identity theft and credit fraud often go undetected. However, the ramifications of the crime can have serious long-term effects on your finances.

While the methods of credit monitoring have improved, most perpetrators of identity theft and fraud are caught after the fact, not during or even before the crime. Most people don't find out that they are a victim until their credit has been violated. And by then the damage is well underway.

Such time lapses can worsen the damage, adding to the dollar and time costs to both affected businesses and victims. According to various reports, actual losses from an average identity theft crime are around $6,000, and anywhere from $400 to $800 of that comes out of the victim's pocket. Victims report spending at least 40 hours over many months dealing with the administrative hassles of the crime.

Fixing the signs of credit crime isn't optional, either. Your most valuable personal asset is your reputation, and the only way bankers, employers, landlords, creditors, and others have to measure your money-handling ways is your credit file.

David and Tom Gardner recently sat down with Dayana Yochim, The Motley Fool's long-time credit watchdog and personal finance guru, and Shannon Zimmerman, mutual fund expert and electronic password-protection aficionado. They talked about dumpster divers, pickpockets, online scammers, and everyone else who may want a piece of your personal credit file. Below, they tell you how to thwart thieves and take back your good name if you do fall victim.

David Gardner: How bad is the identity theft/credit fraud problem anyway? Is it really something that I need to be concerned about?

Dayana Yochim: The Federal Trade Commission reports that identity fraud — that's when someone opens new accounts in other peoples' names or accesses and uses existing accounts — affects approximately eight to 10 million Americans each year. That's about 4% of the population.

But if you follow the headlines, you might be led to believe that identity theft is running rampant and unchecked through the streets of every town. The truth lies somewhere in between.

The chances are relatively small that you will become a victim of identity theft or credit fraud. In fact, a recent study showed that in 2005, identity fraud crimes actually went down. However, the chances that your personal data will be compromised is not slim. And that's the real issue: information security. That's what we should all be up in arms about.

The real story behind the blaring identity theft headlines is information security. That's what we should all be up in arms about.

In recent memory, we've seen ChoicePoint unwittingly allowing fraudsters to access 144,000 private files; a breach at LexisNexis exposing info on 300,000 consumers; Time Warner losing backup tapes with background data on 600,000 current and former employees; and customers of Marriott, BJ's Wholesale Club, and — one that hit a little too close to home for me — shoe-superstore DSW — all getting hacked.

But hacking's only part of it. Some companies have been downright careless with the information we've entrusted them to keep under wraps. Just before tax season, H&R Block sent out a promotional offer with free tax-preparation software. Some of the mailing labels had the recipient's Social Security number printed right on the package. Now, in that case, a crook would have to know what he was looking at since the numbers weren't obviously labeled. Even so, careless handling of such sensitive data should be cause for serious alarm.

So to answer your question: Are you going to be a victim of identity theft? Probably not. Will unscrupulous people get access to your personal data? Better plan on it.

Tom Gardner: What do companies do when such a breach occurs?

Dayana: Here's what happens: The data that the company insisted that you provide to them — information like your Social Security number, address, favorite color, whatever — is somehow breached. Victims are notified, usually by letter, and in many instances, they are given a free subscription to a "credit watch" program offered by a third-party vendor such as one of the credit bureaus.

Frankly, I don't think that's an adequate response. By the time someone is alerted to fishy activity in their credit file, they are already a victim. It's also unclear how quickly victims are notified. In the case of the recent VA breach, the thieves got a huge head start over the credit cops. The Justice Department wasn't even told of the theft until two weeks after it took place.

Some companies put "fraud watches" on consumer files. That's like a lock on a person's credit. With a fraud watch in place, creditors must contact the consumer directly when any new lines of credit are requested. It prevents bad guys from using your name to get credit, charge cards, or loans, but it can be inconvenient for anyone in the midst of shopping for a loan, refinancing a house, or getting a credit card. Plus the fraud watch is only on your file for a limited amount of time.

David: Is it just big companies who are exposing your data? Or do you have to watch out when you're shopping online?

Dayana: The Internet has gotten a bad rap when it comes to identity fraud. Most people assume that the

majority of crimes are committed by strangers stalking you online. But a recent study found that about 90% of thefts take place offline via old-school crimes like wallet or purse-snatching and mailbox theft.

Even more shocking is that nearly half of all identity thefts are committed by someone the victim knows, which makes sense given the access that roommates, family members, friends (or, I should say so-called friends), and acquaintances have to all the information needed to perpetrate the crime.

The elderly are often targets, but so are younger folks. The most common victims are those in the 25- to 34-year-old age group. And while it may feel weird to narc out someone you know for committing fraud in your name, remember that no one has the right to rip off a loved one or a friend.

David: How do you keep from being an unwitting victim?

Shannon Zimmerman: As in other areas of life, early detection is key. Prevention is the preferred method of dealing with identity theft and credit. The best way for consumers to use the credit monitoring system is to keep tabs on what's happening in their credit files on a regular basis.

By law, all U.S. consumers are allowed a free copy of their credit report once a year from the three major reporting bureaus — Equifax, TransUnion, and Experian. You can get yours by going to www.annualcreditreport.com. If you order your Equifax report in January, then you should mark your calendar to order your TransUnion or Experian report the next quarter and so on. You'll then be monitoring your credit activity on a pretty regular basis at no cost.

However, this isn't a bulletproof system. That's because not all reporting entities share information with all three of these credit bureaus. So activity on one report may not show up at all on another. But if something fishy were to turn up, you would at least know to check your other reports. And when fraud is suspected, consumers are entitled to a free credit report.

If you really want to stay on top of all the activity in your file, you can subscribe to a credit-watch program that sends regular updates on any credit activity in your name, including new accounts, changes in your credit limits, and credit usage.

Check Your Credit for Free — for Real!

Three cheers for FACTA! Fact-huh? That's FACT Act, which stands for Fair and Accurate Credit Transactions Act. It's part of the Fair Credit Reporting Act, which regulates how your credit information can be used.

But all you really need to know is that every 12 months, everyone in this great land of ours is entitled to a free credit report from each of the three major credit reporting agencies. The free reports do not contain your credit score; instead, you get the three-digit "credit GPA" that each bureau assigns to you.

The Federal Trade Commission is still determining a standard price that credit reporting agencies can charge consumers for their scores. The final price should be between $4 and $8.

David: What do people do when they steal your identity?

Dayana: TV dramas have been great about highlighting the most dramatic kinds of identity theft. "The *real* Billy Smith died in a fiery car crash. The man you're married to is actually *Hal Smythe* — he's been passing himself off as Billy Smith for the past 20 years!"

In reality, people who commit identity theft open credit card, cell phone, or utility accounts fraudulently. They open bank accounts and get loans in another person's name. And in some instances, they even get jobs by using someone else's information.

Credit fraud is different from identity theft. Credit fraud is committed when someone uses your existing credit, card, or bank accounts without your permission.

Tom: If someone assumes my identity, I hope they at least take responsibility for doing the dishes. Until then, how I protect myself from fraudsters who aren't willing to chip in on housework duties?

Shannon: The best way to protect yourself is to make sure you cover all your data security weak spots.

Actually look at your credit card and bank account statements to make sure no funny business has taken place. If a bill or bank or other account statement is late arriving in the mail, call the provider and find out why. You want to make sure that someone hasn't ferreted through your mailbox for personal information. You also should use post office boxes — not your mailbox — for your outgoing mail. And if you're going on vacation, put a hold on your mail at the post office or have a trusted neighbor pick it up for you.

Tear or shred those annoying "convenience checks" your credit card company sends daily as well as any other personal information (receipts, insurance forms, bank statements, credit card offers) that's trash-bound.

Give Trash-Picking Thieves Less Fodder

Take your name off the junk mail lists. Opt out of pre-approved credit card offers — gold to identity thieves — by calling **888-5OPTOUT** (888-567-8688). Buy a cheap shredder, gather any official documents destined for the trash, and pretend you work at Enron during commercial breaks.

Sometimes being too trusting puts your personal data in danger. There have been a lot of instances where people get calls that are supposedly from their credit card company or bank. The person on the other end of the line knows just enough about you and your account to be believable. Then they'll fish for just one last piece of information, telling you that your account has been compromised. Since you want to protect yourself, you'll give them the extra info they need — like a password or your mother's maiden name.

Never give out personal information over the phone, through the mail, or online unless you initiate the contact or know the caller. Thieves will pose as bank representatives, Internet service providers, government agents, and ex-boyfriends to get you to reveal personal information. In fact, if you get such a call, ask for the person's information and then hang up, get out your account statement, and call the institution yourself.

Don't give out personal information on the phone, through the mail, or online unless you initiate the contact or know the caller.

Dayana: Put another way, just follow the advice the district attorneys on *Law & Order* give witnesses about to face the defense attorney: Never give out more information than you're asked to.

So when it comes to protecting your identity:

- Don't carry your Social Security card with you. Stash it in a safe place.
- Don't lug around cards or IDs you don't need or use on a regular basis.
- Don't pre-print your Social Security or driver's license numbers on your checks.
- When you're asked to provide your Social Security number, ask if another identifier is acceptable.

I often advise people to take a break at work and Xerox the contents of their wallet — front and back — and then keep a copy in a safe place at work and one at home. That way you have the vital information (customer service phone numbers, card numbers) if your wallet is stolen. But don't blame me if you get in trouble for using the copy machine for personal business!

Sadly, this is only a partial list of protective measures. If you're really paranoid, make the FTC's ID theft website (www.consumer.gov/idtheft/) your home page. It's regularly updated with the latest scams.

Mailbox Watch

Christmas for fraudsters starts in January. That's when information-rich tax-related documents begin to snake through the postal system.

According to CNET, about 8% of identity theft cases are linked to mailbox breaches. Keep a watch on your paperwork: On the outside of your "2006 Taxes" folder, keep a running list of everyone who pays you (for work, interest, etc.).

Check off the names as soon as you receive a copy of what they filed with the IRS. Track down missing docs by mid-February by contacting the original source.

David: Let's turn to one of the more vulnerable places of attack — our computers. What should we do to ward off hackers and "phishing" attacks?

Dayana: Don't click *anything*. Ever.

OK, since that's not really a workable option for most, there are a few basic things you can do to keep from being electronically compromised. The most common kind of cyber crime is "phishing" — that's when a scammer mimics a legit organization via email or an instant message to trick victims into revealing account details or other personal information. "Pharming" exploits vulnerabilities in DNS servers (with a virus or script hidden on a page) by redirecting a victim's browser to a look-alike website.

These scams run the gamut from extremely unsophisticated instant messages or spoof emails riddled with grammatical errors to amazingly professional websites that look nearly identical to the real deal.

Shannon: To guard against cyber-crime:

Password-protect everything. Use a complex assortment of nonsensical letters, numbers, and random punctuation marks. And don't just use your dog's name. Trust me.

Don't put the good stuff on a handheld device. If Paris Hilton taught us one important lesson it's this: Don't put any sensitive info on your handheld device. And if you must, handcuff it to yourself. If you lose your PDA, having your Social Security number and a list of bank and brokerage accounts on it only compounds the potential damage.

Seriously, don't click *that*! We've all gotten those emails from banks we don't even do business with telling saying that there's a problem with our nonexistent account. Ignore the solicitations.

See if anyone's spying. To guard against the less obvious come-ons, take a tour of your computer to see whether anyone's lurking. The CERT Coordination Center (operated by Carnegie Mellon University) has a library of Internet security tips (www.cert.org/tech_tips/) — from installing initial security measures to responding to incidents and fixing email abuses.

Phishing can also happen offline, as Shannon mentioned, when a thief gets information about where you bank or do business and then calls and tries to get additional information from you — such as your password. Again, hang up and initiate the phone call directly with the financial institution yourself.

Tom: OK, say I've done everything I can to protect myself. How can I tell if my identity has been stolen or someone is monkeying with my financial identity?

Dayana: I've written about this topic a lot on Fool.com. There are seven main things that serve as potential warning signs.

1. Strange charges on your credit card or bank debit card statement. This is why — and I know it's a drag — you should actually review your bank and credit card statements each month. This is usually the first place you'll spot unauthorized activity. A friend of mine didn't notice that he was a victim for a few months because the charges on his card were at places like Target, Home Depot, and Petco — all places that he and his wife occasionally shopped. So take a moment to really review the charges.

2. Missing bills. It's not uncommon to misplace a bill. What is uncommon is when several months go by

without a service provider requesting payment. If an expected invoice fails to materialize, that could mean a crook has changed your address. This happened to a man I interviewed a few years ago when he noticed that he stopped receiving statements from his bank about his home equity line of credit. The bank informed him that it had — at his supposed request — changed his address and mailed new checks and all account statements to the Bronx. In the meantime, $90,000 worth of checks had been written against his home equity. This could have gone on indefinitely since the thieves kindly made minimum payments on the account to avoid suspicion.

3. Snubs from lenders. Another sign is if you're rebuffed by a lender to whom you've applied for credit even though you know you're entirely creditworthy. So check your credit reports quarterly for free at annualcreditreport.com, as Shannon pointed out earlier.

4. Brain freeze at the ATM. When your PINs and other access codes stop working, that may mean that someone changed the codes on you.

5. A case of mistaken identity. Not all identity mishaps are part of an evil plot to besmirch your reputation. People with common names — or those who are a Jr. or II to a Sr. or I in the family — often find other people's information in their file. To prevent this from happening, make sure to always use your middle name or initial on applications.

6. Dramatically different credit scores from bureau to bureau. Occasionally, a big difference — say, 50 points or more — in your score from one credit reporting agency to another may be a sign that something's fishy. However, don't immediately assume that something's amiss. There are a lot of reasons your credit score might seem wacky, some of which are quite innocent. Not all lenders report all account activity to all three credit bureaus. So an account opened in your name may not be on everyone's radar.

7. Angry phone calls. If you're not in the habit of skipping out on financial obligations or bouncing checks and you start getting calls from collection agencies (usually during the climax of *Grey's Anatomy*), you might have a problem. A co-worker found out about a bank account opened in his name when he got a call from Lowe's about a $1,000 bounced check he didn't write. If this happens, gather all the information you can from the demanding party and start investigating.

Credit Info Overload

Approximately 100,000 entities report information to the credit reporting agencies. That includes lenders, collection agencies, credit card companies, leasing firms — anyone who extends you credit or reports information about you.

Currently, 2 million credit reports are ordered each day, and 2 billion pieces of information are added to these files each month.

David: What should I do if I find out that either my identity has been stolen or credit fraud against me has happened?

Shannon: Since I like to play out these "just in case" scenarios for my own peace-of-mind, let me field this one. If you are a victim, here's what to do:

1. Report the theft to the major credit bureaus (they all have fraud centers). One toll-free phone call to any of the nationwide credit reporting companies will start a chain reaction of protection measures with all of them. By notifying the agencies as soon as you discover the fraud, you can reduce the chance of further credit shenanigans in your good name. Ask that a fraud alert be placed on your file and request that no new lines of credit be opened without your express approval. You may be asked to record the incident(s) in writing and include copies of any documents (e.g., a police report, correspondence with your bank or other creditors) to be used as evidence.

Within 24 hours of making the call, a fraud alert will be placed on the credit files, you'll be opted out of pre-approved offers for credit or insurance for two years, and a copy of your credit file will be sent by one of the agencies within three business days.

After that, credit reporting companies will work with you to verify the information in their respective reports and delete any fraudulent data. Filing a police report will accelerate the process. Members of the Consumer Data Industry Association will immediately delete fraudulent data without the usual reinvestigation procedures.

Make Creditors Call You Before Any Funny Business Occurs

Ask the credit reporting agencies to put a fraud alert on your file. (By calling one, all three will comply.) It requires lenders to request additional documentation from you any time you request credit.

If you get a call about a credit application you didn't fill out, you can stop a thief in his tracks. It will also opt you out of pre-approved offers. Fraud alerts expire, so make a note of when you need to re-up.

Here are the contact numbers:
Equifax: (888) 766-0008
Experian: (888) 397-3742
TransUnion: (800) 680-7289

2. Close accounts that have been fraudulently accessed or opened. To do so, contact the security departments of the appropriate creditors or financial institutions. If you open any new accounts, put passwords on them.

3. File a police report. Be sure to get a copy of the report (or report number) in case the bank, credit card company, or others need proof of the crime.

4. Be a tattletale. The FTC provides an ID Theft Affidavit (www.consumer.gov/idtheft/) that can help you organize and accurately record your complaint. All three major credit bureaus and most major lenders accept this form as notice from you. You can also call the ID Theft Clearinghouse toll-free at (877) ID-THEFT (438-4338) to report the theft. For more information on how to deal with credit-related ID theft, check out the ID Theft website (www.consumer.gov/idtheft). If the crime involves your Social Security number, call (800) 269-0271 or visit the Social Security Administration's website (www.ssa.gov/).

Tom: Is it possible for someone to wreck your credit without stealing your identity?

Dayana: Absolutely. Just ask anyone who has shown their boundless love for another by intertwining their financial lives and then discovering that their sweetheart or son or daughter wasn't so great about paying the bills on time. When you jointly hold credit, the good and the bad (the little flubs like paying bills late or big ones like defaulting on a loan) appear on both of your credit reports.

I've heard from many readers who have discovered after a divorce that their ex had abused joint lines of credit or even opened new lines of credit without notifying them. Banks don't care why your union went awry or who is really responsible for paying the bill. They just want to get paid.

These kinds of problems can come up years after the fact, too, when a charged-off account is sold to a collection agency and they start calling demanding payment. The best thing to do in that case is to get copies of your credit reports and see what's being reported and by whom. You may also have to contact your ex to get the issue resolved. There is a statute of limitations on how long some bad marks can be reported to the credit bureaus, so you also want to make sure that the bill collectors are operating within those legal limits.

David: What if a family member — say, your kid in college — needs access to a line of credit but either can't qualify for it on their own or isn't ready for the responsibility?

Dayana: If your loved one needs access to a line of credit but you don't want to risk having their mistakes mar your record, I suggest making them an authorized user on your account. You can even separate tabs by having an account just for their use. The card is in your name and you are solely responsible for the charges. However, when or if it comes time to sever those credit ties, it's a lot easier to remove an autho-

rized user from the account than it is to close a joint account, particularly if the other person is reluctant to do so.

Tom: How do these identity/credit scams affect your investments or ability to invest?

Shannon: If your identity is compromised, the bad guys could gain access to your brokerage accounts in the same way they can access your bank accounts and credit cards. The worst-case scenario is that the thief could change the mailing address on your brokerage account, sell your stocks, liquidate the funds, and empty your account.

Having your identity stolen also ties up your assets, at least for a little while. Say the thief empties your bank account — while most banks won't hold you liable for the stolen or fraudulently accessed money, the hassle of having your accounts compromised can put a serious cramp in your investing ability. If you don't catch the crook in a timely manner, you could bounce checks, be short on your mortgage, have to stop automatic investing transfers — all things that complicate getting your credit reputation back on track. And while you are putting your time, energy, and money into recovering from the identity theft, you'll have less time to focus on your finances overall. So, in short, follow the tips we've talked about to prevent identity theft from happening to you.

This has been the third and final installment of The Motley Fool's "Master Your Money" series. If you missed the two previous offers, fret not. They are still available for free!

- To access "12 Investing Secrets Corporate America Doesn't Want You to Know About," just click (or type) this link: http://www.fool.com/m.asp?i=2049862.
- To download an audio file of "How to Know When to Buy or Sell a Stock Regardless of Whether You Are a Seasoned Pro or a Rookie Investor" where Dayana and Shannon interview David and Tom, just visit our blog at: www.MasterYourMoneyBlog.com.

We'd love to hear your comments about identity theft, investing, and any other money matters. Head to www.MasterYourMoneyBlog.com to peruse and post and tell us what's on your mind. Simply look for the post titled "Protect Your Foolish Identity" and let us know what you think by leaving a comment or a question.