

Internet Scams for 2006

Trading Tips: This scam passes itself off as an "insiders tip" to stocks that are supposedly going to "explode". The premise is that they will get you more money for your portfolio if you agree to call them, email them or contact them some way and give your credit card number for transactions.

Internet Lottery: So, you've won ONE MILLION PESOS!? Not so. These emails are nothing but a scam to get you to give your bank account information to would-be thieves so they can infiltrate your account.

Internet Job Offers: If an email ends in "This is not a scam".....it probably IS a scam. Many times would be internet prey will receive an email telling them that they are being offered a very lucrative job. More likely than not, the "employer" will request cash (in the form of a credit card payment or automatic withdraw from your bank account) that will entitle the "employee" to data bases to be used for work at home making "\$1,000.00's of dollars per week".

Phishing scams: Phishing scams are clever and complex ways to get your information to identity thieves. These scams are more readily known as

the "Dear Customer, we had to block your account due to....." scam. "Phishers" will also ask for information such as your log on name, password, etc. The most common Internet users targeted by phishers are Ebay and Paypal users. Remember that if you do receive an email from Paypal or Ebay, they will always use your first name. These scams even go so far as to use trademark symbols and/or what appears to be email account information from any number of financial institutions, reputed service providers, etc. A study done last June by Gartner Inc. showed that about 2.4 million people in the US reported losing \$929 million through phishing scams during the previous year.

Slain Foreign Diplomat Family in Crisis: These emails appear from any number of "foreign diplomat family members" claiming something to the effect of "if I don't receive \$x,xxx,xxx.xx within the next few days, they will kill me too" or "I need to hide a bazillion dollars in your bank account". Like all con games, be they online or in person, the con man is trying to get you to entrust him with your cash or access to your cash.

As with any email you may receive that sounds too good to be true, it probably is. Mom was right!

You can check any email that you find suspicious as to its authenticity at www.scambusters.com.



The

Legal-E-Z

October, 2006 • Vol.1 Issue 2

THE LAW LIBRARY
J.V. Brown Library
19 East Fourth St.
Williamsport, PA
570.326.0536
www.jvbrown.edu

Sheri Crain
scrain@jvbrown.edu

NOTICE:
Nothing in this publication is intended to be legal advice. If you desire legal advice, you must hire a private attorney.

In this issue : Identity Theft. Look for specialized articles in future issues.

The Law Library at the JVBLibrary is open to the public and is to be used as a reference tool for those seeking information about legal options.

"Identity theft is one of the fastest-growing crimes in the nation - especially in the suburbs."

Melissa Bean

identity theft

Function: *noun*

the illegal use of someone else's personal information (as a Social Security number) in order to obtain money or credit



Identity theft involves a person illegally obtaining and using your personal data. Names, addresss, telephone numbers, credit card numbers, mother's maiden name, and social security numbers are several of things that are used to commit identity theft, most often in the form of financial deception such as opening a new bank account, buying something on your credit accounts or actually obtaining new credit in your name. The identity thief normally intrudes with the intention of obtaining goods and/or services in your name, ultimately wanting to leave you with the bill!

Identity thieves show no bias toward victims. They are as likely to target those who have well-established credit as well as those with not as much credit, such as college students, and set up fake credit accounts in their names.

Students tend to make relatively easy targets as their information is often easier to obtain (especially if they attend a school that continues to use their social security number as their identification number) and many don't closely monitor their financial accounts, although they receive credit card applications by mail on a regular basis.

In this issue of The Legal-E-Z, we'll explore forms of identity theft, ways to prevent being a victim and what you can do if you find that you ARE a victim.



Continued p.2.

What do many people have in common with: Tiger Woods, Oprah Winfrey, Martha Stewart, Warren Buffet, Tom Cruise

All are/have been victims of identity theft!!!

Here are some tips on how to protect yourself:

1. Your wallet: a wealth of information

Carry only the cards you actually need.

Do you really need to carry your:

1. Social Security Card?
2. ATM Card?
3. Credit Cards?
4. Checks?

2. Make it unique:

Choose a Personal Identification Number (PIN) that is different from:

1. Your phone number
2. Digits in your Social Security Number
3. Address
4. Birth Date

3. Change passwords frequently

- Don't use your pet's name or spouse's name
- Don't use any part of your birth date, address or social security number
- Don't use words found in the dictionary
- DO use a combination of letters and numbers (example: House4saLe)
- DON'T OPT TO "SAVE PASSWORD" FOR AUTOMATIC LOGIN TO WEBSITES

4. Keep it in mind

- Memorize your PIN and Passwords
- Do not write your PIN on your card
- Do not keep PINS or passwords in your wallet

5. Watch your back

Be aware of people who are eavesdropping or watching you enter your PIN

6. Shred the evidence

- Invest in a reasonably priced paper shredder
- Choose a shredder that "crosscuts" as opposed to "straightcuts"

7. Preapproved credit card offers are easy targets

- Call 1-888-5OPT-OUT (1-888-567-8688)

8. Yearly credit reports

- One annual credit report free
- Annual credit report request
 - Online: www.annualcreditreport.com
 - By telephone: 1-877-322-8228
 - By mail: Annual Credit Report Request
P.O. Box 105283
Atlanta, GA 30348-5283

9. Collect your mail

Do not leave mail in your mailbox overnight or on the weekends. Thieves can change your billing address and take control of your accounts(s).

10. Don't give out your Social Security Number

Do not give out your SSN, credit card numbers or bank account numbers unless you know who you are dealing with and it is for a good reason and is required

Many institutions and insurance carriers now issue ID numbers rather than using Social Security Numbers

11. Look for the lock *(the little padlock at the bottom of your computer screen that should be present before you proceed with any online transaction)*

- Don't provide unnecessary information
- Keep a low profile online to reduce your risk
- Opt not to be included in directories
- Look for the padlock!
- Ensure a secure connection with the server

12. Keep software updated

- Update computer software
- Get all the latest security patches
- Get virus protection
- Install a firewall

13. Discarding your computer

- Disc shredders
- Wipe your hard drive clean before you throw away, give away or sell.
- BCWipe www.jetico.com
- Meets Department of Defense computer security standards
- WipeDrive www.whitecanyon.com

If you become a victim:

1. Contact the 3 major reporting agencies
2. Contact the creditors or banks for any accounts that may have been opened, tampered with or opened fraudulently.
3. If you know where the theft took place, file a report with the local police in that community.

IDENTITY THEFT RESOURCES



Thomson Gale LegalForms

Online access to professional legal documents for critical life issues, including:

Bankruptcy • Contracts • Divorce
Employment Incorporation
Landlord/Tenant Agreements
Living Wills • Name Change
Power of Attorney • Real Estate Taxes
Last Will and Testament
And many more

Accessible and downloadable at
www.jvbrown.edu

Annual Credit Report Request

Online: www.annualcreditreport.com

By telephone: 877-322-8228

By Mail: Annual Credit Report Request

P.O. Box 105283

Atlanta, GA 30348-5283

Note: Reports are free. If you are requested to pay for this service, you are not at the official location.

Banks and Checks

To determine if someone has opened a bank account in your name, contact Chex Systems, Inc.

Online: www.chexhelp.com

By telephone: 800-428-9623

By fax: 602-659-2197

By mail: Chex Systems, Inc.

Attn: Consumer Relations

7805 Hudson Road, Suite 100

Woodbury, MN 55125

Action for lost or stolen checks:

1. Stop check and/or close accounts
2. Ask bank to notify Chex Systems, Inc. This service notifies businesses not to accept checks on the flagged account.
3. Notify TeleCheck; this service notifies retailers who use their databases not to accept your checks. The number for TeleCheck is: 800-710-9898 or 800-972-0188
4. Contact SCAN to determine if checks have been passed at 800-262-7771

Bankruptcy

To determine if someone has filed for bankruptcy under your name, contact the U.S. Trustee where you think the bankruptcy has been filed. A list of U.S. Trustees can be found at www.usdoj.gov/ust

File a Complaint with the Federal Trade Commission (FTC)

Online: www.ftc.gov

By telephone: 877-438-4338

By mail: Identity Theft Clearing House
Federal Trade Commission
60 Pennsylvania Avenue
Washington, DC 20580

Other resources:

www.consumer.gov/idtheft

www.privacyrights.org

www.identitytheft.org

Credit Reporting Agencies

File a fraud alert with the three major credit reporting agencies. Call one of the numbers listed below. The company you call is required to notify the other two.

Equifax: 800-525-6285 or

www.equifax.com

Experian: 888-397-3742 or

www.experian.com

TransUnion: 800-680-7289 or

www.transunion.com

National Do-Not-Call Registry:

888-382-1222

PA Do-Not-Call Registry:

888-777-3406

Postal Fraud

Report to local Postmaster

Opt-Out of receiving offers of credit in the mail:

888-567-8688

Social Security Number Misuse

Online: www.socialsecurity.gov/org

By telephone: 800-269-0271

The Story of Bronti Kelly

For four long years, Bronti Kelly couldn't figure out why no one wanted to hire him. He handed department store managers across southern California a resume full of sales experience, but was rejected hundreds of times.

Those rare time when he got a job, he would be fired within days. Along the way, Kelly filed for bankruptcy, lost his apartment, and became homeless. "For years as this went on, I blamed myself—for not being hired for employment, the conditions I went through," Kelly says. But Kelly's self-blame turned to anger when he finally learned the real cause of much of his trouble: A man had given Kelly's identity to authorities when arrested for shoplifting and other crimes, and the tainted profile found its way into a range of computer databases used in background checks by employers.

Kelly's plight illuminates the growing threats to privacy in an age of ever easier computer access to public information.

Bronti Wayne Kelly, now in his 30's, hardly foresaw the cyber nightmare that would grow from what seemed an old-fashioned wallet snatching in May 1990. He reported to police his wallet only contained \$4.00, along with his driver's license, social security card and military ID for the Air Force Base in southern California, where he served as a reservist. But seven months later, Kelly, a salesman in a department store in Riverside, was ushered into the personnel director's office and told he had been caught shoplifting by security guards in another sister department store. Kelly produced a letter from his Air Force commanding officer saying that Kelly was on duty when the crime occurred, but he was fired anyway.

He says he was equally confounded by the blur of job rejections that followed, usually with no explanation.

For two years he held on. Kelly's work as a mechanic at the local air force base earned him about \$700 per month. But in June 1993, the six-year reserve sting was up. With no job in sight, Kelly filed for bankruptcy to stave off bill collectors. He was evicted from his apartment in San Bernadino, California.

Kelly stayed with friends until he wore out his welcome. He turned to sleeping in his car, then the streets, using public parking garages downtown to shield him from the elements.

He tried to keep clean using a pool shower at his old apartment complex.

He applied for food stamps and welfare but was rejected because he had no residence or mailing address. He finally landed a job selling clothes at a department store in nearby Riverside, but the day before his first day of work, he was told that his services were not needed.

Kelly, crying at the news, tried to find out why. The personnel manager told him to contact Stores Protective Association, which exchanges information about employees with more than 100 member retail chains.

Kelly wrote to the company and received a written explanation in January 1995, pegging him for the same shoplifting offense he thought had been purged from the records four years earlier. "I couldn't believe the information was still on file," Kelly said. "I had never even heard of SPA before." But the vast majority of employers Kelly had applied to were members of SPA.

It took until the next month for the association to remove the false information from its files on Kelly, and then only after a local television station reported his woes. A lawyer for SPA, which Kelly is suing in a defamation lawsuit that also names the department store parent, said that Kelly had never given it evidence other than his own statement that he was not the shoplifter.

Kelly is seeking unspecified damages and a public apology from the department store. Kelly's problem was far more complicated than he suspected. When Kelly contacted the Los Angeles Police Department to try and straighten things out, he discovered that its records showed he had been arrested five years earlier not only for shoplifting, but for burglary and arson as well.

Kelly submitted his fingerprints to prove to authorities that he was not the accused culprit, that instead the miscreant was another white male who had given Kelly's identity to police.

The police gave Kelly a "Certificate of Clearance," which states that the police had determined that Kelly was not the person arrested.

However, Kelly's identity remains in police files, even though the most serious charges against the impersonator had been dismissed shortly after his arrest in July 1990. LAPD officials say they need the charges on record in case the impostor is arrested for other crimes.

After SPA removed Kelly's name from its files, he was still rejected from another 50 jobs, and he is still wondering why. One possibility is that the incorrect information continues to haunt him. The problem was spelled out after the Associated Press hired an information search company to conduct a search of Kelly's background. AP simply gave a company Kelly's name, Social Security number and \$124 to search state court records in three counties in southern California.

On a personal note—



As many of my co-workers will tell you, I'm not quick to share personal information, so this is a stretch for me, but I felt it important to share.

A few years back, while enjoying an evening out with some friends, I arrived back at my car to find that my car had been broken into and my purse, which I thought I had so carefully hidden under my dashboard, was ransacked. The thieves apparently forced my locks and then proceeded to dump my purse, and take my wallet, my cell phone and my checkbook. I can tell you it was one of the scariest situations I've been in since reaching adulthood.

After the initial trauma of talking to the police and realizing that there wasn't a lot they could do, I returned home to begin the daunting task of trying to remember exactly what was in my

The search came back showing that Kelly had been arrested in July 1990 for arson, theft and disturbing the peace. But Kelly no longer has to worry. Seven years after his wallet was stolen, he has stopped seeking work among strangers.

He is employed part-time cleaning pools in a family business, and shares an apartment in Temecula, near San Diego, with a roommate who has helped him out financially. Trying to rebuild his self image, Kelly carries his police certificate clearing him of crimes wherever he goes. One look in the mirror confirms it was

wallet, never mind how to contact the different banks, etc.

Luckily, I knew my credit card number by heart (my husband attributes that to me shopping a bit too much) and could immediately call my bank to cancel the card. Unfortunately, the bank informed me that at 1:00 AM, it was impossible to process the request until morning (where I grew up, 1:00 AM WAS morning). Luckily, the only charges to my card were to two gas stations in the area by morning.

What I didn't realize is how incredibly difficult it is to remember everything in your wallet or purse!

Over the ensuing days, I took care of calling my health, vision and dental insurance carriers. I closed out my checking account and opened a new one. Guess what? I was without convenient access to my money for about 10 days. No debit card, no credit card and no checks. Contrary to popular belief, Mortgage Companies do NOT care if your wallet is stolen.

I can honestly say that over the past 2-3 years, I've consistently run into situations where I realize that yet another card is missing. The countless number of grocery store discount cards, the department store discount cards, video club membership cards that have come up missing when I go to use them (hence my counterclaim to my husband's claim that I shop too much—I love creativity). I had to close out my PayPal account, my Ebay account, every online account related to my

not he who dragged down his life. Says Kelly: "A part of me feels very proud." But just to be sure, he is thinking of changing his name.

Bad things can happen to good people, and they do.¹

(Endnotes) ¹ 2000 Associated Press

former bank account. I had to contact the Department of Motor Vehicles to get a new license, I had to change my cell phone number, and I even lost my Social Security Card, my birth certificate and my Passport. I didn't realize my Passport was in my purse, but apparently I had used it recently for identification while registering my son for baseball.

I think that I've finally reconfigured my stolen wallet. I had no money in it, as I put my money in my pants pocket that night, but the things that were stolen caused far more commotion in my life than any amount of money lost could have caused. I can honestly say that I felt violated, dirty, scared, frustrated and sad all at the same time. Someone knew more about me than I would have liked. Someone knew more about me than my closest friends knew! Someone knew more about me than my husband knew!

Today, I have a list of everything that is in my wallet. I have photocopies of the front and back of each card in my filing cabinet. God forbid this should happen again, this time I'll be ready for the process of regaining my lost belongings, but I'll never be ready for the emotional trauma again.

I always said that I'd never be a victim of theft. Not me, I'm immune from that kind of thing. I'll never say never again.

*Sheri Crain,
Legal Reference Assistant
James V. Brown/Lycoming County
Law Library*

ARE YOU AT RISK FOR IDENTITY THEFT

Test your "Identity Quotient"

- | | |
|--|---|
| <p>1.) I receive several pre-approved credit offers every month (add 1 point). (Add 2 more points if you do not shred them before putting them in the trash).</p> <p>2.) I receive several convenience checks in the mail (from credit card companies) every month (1 point) (Add 2 more points if you do not shred them before putting them in the trash).</p> <p>3.) I carry my Social Security Card in my wallet. (3 points)</p> <p>4.) I do not have a locked, secured mailbox or P.O. Box in which to receive mail. (1 point)</p> <p>5.) I leave mail for pick up in an open box at work, clipped to a mailbox or in an unlocked box at my home (2 points)</p> <p>6.) I carry my military I.D. or Medicare card in my wallet at all times. (1 point)</p> <p>7.) I do not crosscut shred banking and credit information when I throw it in the trash. (2 points)</p> <p>8.) I provide my Social Security Number (SSN) whenever asked, without asking how that information will be safeguarded or why it is necessary for them to have it in the first place. (2 points)</p> <p>9.) I dont check for people who might be listening when giving out my personal information. (2 points)</p> <p>10.) My SSN is publicly displayed or used at work or school (timecards, receipts, badges). (1 point for each violation)</p> <p>11.) I have my SSN or my drivers license number printed on my personal checks. (2 points)</p> <p>12.) My SSN is also my drivers license number and I've made no effort to change that. (2 points)</p> <p>13.) I carry my insurance card in my wallet and either my SSN or that of my spouse. (1 point)</p> | <p>14.) I have not ordered a copy of my credit reports for at least 1year. (2 points) (Add 1 more point if it has been more than 2 years)</p> <p>15.) I do not believe people would root around in my trash looking for credit or financial information. (1 point)</p> <p>16.) I am connected to the internet but do not have (or know if I have) firewall software. (2 points)</p> <p><i>Subtract one point from your score for each of the following positive steps:</i></p> <p>17.) I have opted-out of marketing lists through my bank or at the 888-5OPT-OUT number and I keep an eye on my credit cards whenever they leave my hands to avoid skimming.</p> <p>18.) I do not respond to internet scams and hang up on telephone solicitors.</p> <p>19.) I keep personal identifying information in a locked or protected area of my home, one that visitors cant access.</p> <p><i>Each one of these questions represents a possible risk factor or protection against identity theft.</i></p> <p>More than 20 points - You are at high risk. Its recommended that you purchase a paper shredder, become more security aware in document handling and start to question why people need your personal data.</p> <p>10-20 points - You understand identity theft crime trends but still have a ways to go.</p> <p>0-9 points - Congratulations. Keep up the good work and dont let your guard down.</p> <p><i>© I TRC February 2003. All rights reserved. www.idtheftcenter.com</i></p> |
|--|---|

THE HOW-TO'S OF MAKING INTERNET TRANSACTIONS SAFELY

With the holidays looming above our heads, many customers are drawn to the ease of shopping and the ability to compare products and prices online, as well as the impending offers of "free shipping" or "guaranteed to your doorstep by December 25th!".



By using the following suggestions, you can feel comfortable shopping on the Internet. You can be sure your transactions are safe and your credit card information is going only where you intend it.

There are several ways to help ensure safe transactions on the Internet, and more are becoming possible all the time. Some of these include:

- Stored-value cards (cards that you can buy with specified, loaded dollar amounts such as Wal-Mart Gift Cards, I-Tune cards, online services such as Amazon.com gift cards, etc.)
- Smart cards (cards that can act as credit cards, debit cards and/or stored-value cards, such as Visa/MasterCard Check Cards issued by a particular company, such as a K-Mart sponsored Visa/MasterCard)
- Point-of-sale (POS) devices (like your debit card, or online check)
- Digital cash
- E-wallets
- Online payment services like PayPal

The most prevalent method for paying for the things you purchase online is still the credit card. The following list provides some tips on how to make sure your transaction is secure.

- Use the latest version of Internet browser. The program that you use to surf the Internet is called a browser. This software has built-in encryption capabilities that scramble the information you send to a server. Using the most recent browser ensures that the data is protected using the latest encryption technology. This technology also uses a Secure Sockets Layer (SSL), which is an Internet security protocol used by Internet browsers and Web servers to transmit sensitive information. The server receiving the data uses special "keys" to decode it. You can make sure you are on an SSL by checking the URL — the http at the beginning of the address should have changed to https. Also, you should notice a small lock icon in the status bar at the bottom of your browser window.
- Look for digital certificates that authenticate the entity you are dealing with. Independent services like VeriSign will authenticate the identity of the Web site you are

visiting. Web sites that use this service (usually those that sell items or services online) will have the VeriSign logo. By clicking on the logo, you can be assured that the site is legitimate, rather than a clone of the legitimate company set up to collect your personal and financial information.

- Read the privacy policy. The information you enter on the Web site should be kept confidential. Make sure you read the company's privacy policy to ensure that your personal information won't be sold to others. Services like Trust-E review a company's privacy policy (for a fee) and then allow the company to post the Trust-E logo if its privacy policy follows certain industry standards for consumer protection.
- Only use one credit card for all of your online purchases. It makes it easier to follow the transactions if you make more than one at any one particular site.
- Never give out passwords or user ID information online unless you know who you are dealing with and why they need it. Don't give it out to your Internet service provider if you get an e-mail requesting it. This is a relatively recent scam used to access your account and get your credit card number, along with whatever other personal information is there. Remember that sites like amazon.com or ebay.com will always address you by your first and last name in any email correspondence they may send.
- Keep records of all of your Internet transactions. Watch your credit card statement for the charges and make sure they're accurate. Never hesitate to contact your bank if you suspect that something isn't right. Most financial institutions are very well versed in Internet transactions and Internet security issues these days.
- After you've made purchases online, check your e-mail. Merchants often send confirmation e-mails or other communications about your order.