WHAT'S GOIN' ON

BY WAYNE CHUBB

Greetings, and I hope our March "vacation" from the newsletter didn't leave you wondering what to do with yourself. So what can I do this month, you may ask? Well, from cute little teddy bears to large men in skirts, greasers to banjo pickers, and edible weeds to drinkable spices, we got in ALL goin' on! An most of it is a short drive from Sacramento or less.

Spring has sprung, in spite of the wind and rain that I see outside my window (or would, if it weren't midnight), and events around town reflect the opening of gardening season. Start at the **African Violet Show,** with lots to see, do, learn, and buy, at the Sacramento Garden and Arts Center, aka McKinley Park, on April 3-4. The following weekend brings a new show to Cal Expo, the **California State Flower and Garden Show** (think the Home and Garden Show, but better smelling), April 8-11. The **Open Garden** at the Sacto Historic Rose Garden (aka Old Sacto Cemetery) showcases hundreds of roses, and the opportunity to learn from those who know them best. Lots of heritage roses for sale, too. Finish up the month by checking out God's gardening ideas on the **Wildflower Train**, a guided steam train trip through the foothills near the California Rail Museum in Jamestown on the 24th (and again on May 10th).

Along with all that garden greenery comes Earth Day, which is being celebrated at **Earthfest at the Zoo** at the Sacramento Zoo on April 3rd, followed by the **Earth Day Festival** at South Side Park on the 11th and the **Sacramento Green Expo**, another first time, fully Al Gore– approved show at Cal Expo, on the 24-25th.

Want something even greener, that the whole family can enjoy? It's rumored that an asparagus margarita will be a feature of this year's **Asparagus Festival** on the Stockton Waterfront, April 23-25. Other family fare (pun fully intended) this month includes the **ZooZoom**, a 5K, 10K, and kid's run at the Sacramento Zoo (with a free celebration at the zoo for all runners) on the 11th, and **Picnic Day at UC Davis** on the 17th. Picnic Day has been a UC Davis event since 1909, and includes over 150 events besides my favorite, the Doxie Derby. Get there early—seriously. The **Wild West Stampede,** a 10 day event that ends with a PRCA rodeo, runs from April 15-25 in Auburn. Show the kids what Scotsmen wear under their kilts at the **Sac. Valley Scottish Games and Gathering**, one of the largest (and oldest, since 1876) events of it's kind in the US, in Woodland April 24-25. The competitions and music are great, and the food is, well, Scottish. Equally as much fun, and with better food, is **Festival de la Familia** at Cal Expo on the same weekend.

More grown-up fare can be found at the **Bockbierfest,** a celebration of German food and drink at the Turn Verein Hall near Sac State on the 2nd and 3rd. It bridges the gaps between Octoberfests nicely. Balance out the Asparagus Festival with the **Bethel Island Chili Cook-Off** (elk chili, baby!) on the 18th in the Delta near Pittsburg. The biggest wine event of the month is **Passport Weekend** April 10-11 and 17-18), where all the El Dorado wineries put on their best show. It's pricey and crowded, but well done.

Other options include the **Banjo –Rama** at the Red Lion in Sacto (4/9-11), the **International Teddy Bear Convention** in Nevada City (4/9-11), and the **Sac. Dog Show** at Cal Expo (4/15-18). I may miss those. Two ongoing shows we will see are the **Birth of the Hot Rod** at the Cal. Auto Museum and Mission to Mars at the **Aerospace Museum of California** at McClellan Park, two under the radar jewels in Sacramento.

Happy Easter, happy trout season opener, happy River Cats opener, and see you in May!

Preventative Steps to Avoid Identity Theft & Consumer Fraud

BY JOHN JAY PEFLEY, Esq.

Identity theft is one of the most devastating and fastest growing crimes in America today. The Federal Trade Commission received twice as many identity theft complaints last year over 2007, with victims reporting stolen credit cards, drained bank accounts, and unspeakable damage to their credit ratings. It is estimated that ***one out of five Americans***, or a member of their family, will become a victim of identity theft each year. Identity theft accounts for 43% of consumer fraud complaints filed this year, topping the government's list of fraud related crime for a fourth consecutive year.

ID theft criminals are also becoming more brazen with their attempts to carry out large scale, systematic fraud. One of the largest mortgage lenders in the country disclosed in a series of lawsuits that one of its brokers came to work on Sundays and downloaded on a "flash drive" up to 20,000 complete loan files each Sunday and then sold the private information to the global mafias for one primary purpose- to commit identity theft against the unknowing victims.

A common misconception about identity theft is that **"It will never happen to me"**. Statistically this is not the case. Unfortunately, identity theft already affects the lives of millions of Americans and more than half a million are being added each year according to the Federal Bureau of Investigation. Many victims may never discover that they are victims of identity theft until it is too late. Victims may never know that their identity has been stolen until unauthorized transactions appear on their credit card statements or collection notices appear. Victims that do learn the crime has occurred are left with little assistance to pick up the pieces or to pay for the damages: It is truly victims beware!

Restoring your identity and credit can be an expensive and time-consuming process. On average, a victim of identity theft fraud will spend 170 hours researching the crime, 23 months correcting their credit reports, and up to $3,257 in out of pocket expenses to restore their credit and identity. Victims are urged to report these matters to the authorities as soon as possible. Failure to expediently report identity theft could result in additional damage to a consumer's credit and can decrease their chances of recovery.

The most common form of identity theft is unauthorized use of name, social security number and other data to fraudulently obtain credit cards and open bank accounts.

So how do identity thieves get your personal information?

- They steal wallets, mail and rummage through your trash.
- They complete change of address forms to divert your mail.
- They use your personal information found on the Internet or pose as employers or creditors to obtain copies of your credit report.
- They also obtain credit card slips that you leave at restaurants or throw away.
- They scam you through email ("phishing") or telephone solicitation posing as legitimate companies.

What can you do to avoid loss of identity theft? Here are some preventative steps:

ID Theft Prevention

- **Check your credit report** once a year from each of the three major credit-reporting agencies: Equifax 1-800-685-1111, Experian 1-866-200-6020 and Trans-Union 1-800-888-4213. Do it free every (4) months by rotation at www.annualcreditreport.com.
- **Guard your Social Security number.** Do not give it out, use it as a password for your computer, or put it on your checks, or have it on your driver's license. It is also a good idea not to carry your SS card in your wallet.
- **Maintain careful records** of your banking, credit card and financial records.
- **Be aware of people** who might try to eavesdrop on information that you give out orally; beware of those looking over your shoulder at banks and stores.
- **Carefully destroy and/or shred papers** you dispose of if they contain sensitive information. Invest in a crosscut shredder.
- **Be suspicious of unsolicited** telephone calls or spam-email requesting personal information for unbelievable offers (or "protecting your account"), including lottery or sweepstakes ploys. Hang up quickly; this is the best defense.
- **Be cautious about missing** mail and bills. If your bills do not arrive on time, make sure to report the matter to the appropriate billing company. Open and review all statements promptly upon receipt; look for unauthorized charges.
- **Guard personal account passwords.** Don't use your mother's maiden name, your birth date, or the last four digits of your social security number for passwords.
- **Verify all websites for authenticity** before you make a purchase online using a credit card. Many websites now register their authenticity with third parties such as VeriSign.com or Truste.org for this purpose. Know the vendor!
- **Enroll in a Credit Monitoring and a Fraud Resolution program** through a membership association, your employer, Employee Assistance Program or directly. These organizations can expedite reporting identity theft matters and save you a tremendous amount of time and money. Think of it as a smoke alarm on your credit reputation.
- **Get a locking mailbox**; deliver all mail and bills directly to a Post Office Box.
- **Know what is in your purse or wallet.** Photocopy both sides of your credit cards, insurance cards and driver's license. Store them in a safe place in the event your purse or wallet is stolen. Remove all unnecessary information when traveling.
- **If you have workers or maids** coming to your home for any reason, remove or store all papers and sensitive information to

a safe, inaccessible place.

If you think you are a victim of identity theft or consumer fraud, please report the matter to the authorities and call your member services department if you are enrolled in a membership program that has Identity Theft protection as a benefit. There are many Identity Theft programs that provide you the assistance of a trained Fraud Resolution Specialist™ who can help you to restore your good credit and identity.

Internet Shopping Tips

- Before you input your personal information onto a business' web site, call information and get the business' phone number. Call the business and verify that they do indeed have this website, and that the one you are looking at is indeed legitimate. There are many fake websites out there set up to look just like the real thing.

- Review the privacy and security policies of the companies you do business with. Ensure that you are shopping at a secure website. A secure website uses encryption technology to scramble the information you send. Secure Website addresses also include https:// at the beginning of the address. The "s" indicates the address the Web site is secure. Also look for a closed padlock at the bottom of your screen. If that lock is open, it may be a sign the site is not secure. Double click on the padlock and it should show who the issuer of the security certificate is and it's effective and expiration dates. Never enter personal information if you have any doubt that the site is not secure.

- Be aware that international standards may differ. When you shop in the United States, you are protected by Federal and State consumer laws, which may not apply if you place an order internationally. If it is not a reputable merchant, it may be difficult to resolve the issue. Always print copies of terms, conditions, warranties and company information to use as proof of purchase.

- Never use personal information for passwords. If you use information such as birth dates, names, email addresses or telephone numbers as passwords, it can make you much more susceptible to identity theft.

- Do not respond to "phishing" ("confirming" private data) emails. Even if it appears to be a store or business that you frequently do business with, many of these are designed to get your personal information and may take you into a website that looks real, but is in reality a fake.

Top Things you can do for Computer Safety

Choose a new / better password: Odds are good that you have been using the same password for quite awhile now. Odds are also good that your password is somehow based on your name, your child's name, your social security number, etc. Now is a great time for you to resolve to use stronger passwords to protect yourself and your data.

Keep your system patched: Vulnerabilities are discovered all the time in operating systems and applications. If you subscribe to an email distribution like Bugtraq, or turn on features like the Windows AutoUpdate you can stay in touch with what is going on and know when new patches are available that you should apply to your system. Managing and maintaining current patching is a full-time job for some network administrators.

Install and update antivirus software: New viruses, worms, Trojans and other malicious code are discovered every week and sometimes every day. It is important that you not only install a good antivirus software package, but that you check with the vendor on a weekly basis for any updates to the virus definitions and apply those as well. If you don't keep your antivirus software updated you may as well not even have it installed.

- **Install a personal firewall application:** If you keep your system patched and your antivirus software updated you can rule out many of the threats to your system, but there are a number of other ways your system can be compromised. By installing a personal firewall program you can block unwanted traffic from entering your computer and many of the applications will also monitor how your programs interact with the operating system to alert you when you might be infected with a Trojan as well.

- **Don't open unknown file attachments:** Malicious programmers try to come up with the best subject lines and message bodies for the emails they use to propagate their viruses, Trojans and other malicious code. Many times the email is in broken English that makes no sense in which case it should be obvious that you should delete it without a second thought. But, even if the message makes sense you should think twice about opening any file attachment you don't 100% know the origin or contents of.

- **Use encryption:** Even if an unauthorized person were to somehow gain access to your computer or network, you could further protect your personal or confidential data by encrypting it. Using the built-in EFS (Encrypted File System) in the more recent versions of Microsoft Windows you can encrypt your files or folders so that only you can view them. You might also consider encrypting your email so that only the intended recipient can view it.

- **Back up your important files:** Defining "important" is in the eye of the beholder. For some that may only mean their financial records- bank account files, stock tracking data and such. For many it will also include photos, songs and documents that would be irreplaceable if something were to happen to the computer. Backing up your data is just good common sense. Even if no malicious code, worm, virus, Trojan or otherwise ever infiltrated your computer sometimes hard drives simply crash. You should set up a periodic schedule to back up your data- daily, weekly, monthly or whatever suits your needs best. It is also good practice to take your backup media to another location. If a fire or other physical tragedy should destroy your computer it won't work very well to have the backup files get destroyed at the same time.

- **Take a class:** If you want to get serious about computer and network security you should consider taking a class. There are many offered ranging from the general and basic to the specific and advanced. You may even consider becoming certified in one or more aspects of information security.

- **Read, read and read some more:** There is absolutely no shortage of resources to read that will help you learn more and broaden your horizons when it comes to computer and network security.

John Pefley, Esq., is an attorney with over 32 years of litigation and business experience. He serves as In-House Counsel and as the National Director of the Fraud Resolution Response Unit of CLC Incorporated 800-706-5749. For further ID Theft protection enroll in MSA ID Protect Identity Monitoring today. www.msaidprotect.com

The Chubb Law Firm

11211 Gold Country Blvd, Suite 101
Gold River, CA 95670
916.635.6800

INSIDE THIS ISSUE:

Did you miss me? No, it wasn't your imagination, you didn't receive a March newsletter because I was too busy picking out, installing and learning my new office computer system to get the newsletter together.

Both my computer and Cheryl's computer were poised for catastrophic failure and we had to do something fast. Well, my computer had been dying a slow, painful, and loud death for several months, but when we discovered that Cheryl's system was also dying I knew we were in big trouble. So I did what anyone would do—I jumped ship and bought some iMacs. Now, Cheryl looked at me like I had rocks in my head when I told her I was considering the switch—why change to something new when we know the old stuff? A perfectly good question, to which I had a perfectly good answer—I'm tired of trying to cobble together PC stuff, hiring IT consultants that seem to only know marginally more than I do and always having stuff that needs tweaking.

I have to admit that once I bought the iMacs I did have some panicky moments, especially when I realized I forgot to determine if our current printer and scanner would actually talk to the Macs (they do, but in a little different way than we were used to). We're working out the kinks and keeping our brains sharp by learning new things everyday. I'm pretty sure it will be worth it in the long run, but for now I feel like I bit off a little more than I can chew.

All my best,

Heather