UASFAA Newsletter

Spring 2005

President's Message

by Cristi Easton

Recently I was returning to Salt Lake from Chicago, where I had attended DOE Training of the Trainers. As I was flying in, I wasn't really paying attention to the scenery – after all, I had seen it before. Several people on the side of the plane facing the Wasatch Mountains were exclaiming over the beauty of the mountains. In fact, several people were taking pictures! I was reminded of what a great place Utah is and how fortunate many of us are to work here. Whether we are in Cache Valley, Salt Lake Valley, "Happy" Valley or the red rock of Southern Utah, it's quite spectacular.

Not only do we have a great state to look at, but we also have great peers and co-workers. I have now worked at Salt Lake Community College for 16 years in June. I appreciate, so much, the people within my office. They are supportive, intelligent, hard-working and fun. From talking to many of you, I know your offices are much the same. We are also fortunate to have great peers throughout the state. Although I haven't worked for Mike Johnson in years, I still call him with questions about regulations. I know if I am confused about how to take care of a certain student, I can call any of you in any office and get immediate feedback. Sometimes you laugh at me, but I don't mind! At least I've given you a chance to smile.

As I begin this year as President of UASFAA, I ask all of you to remember what a fulfilling field we work in. Although we may complain about the changing regulations or Congress or even the State Legislature, we have the opportunity to help students fulfill their dreams. We are giving them a chance to become something they may have dreamed about. To illustrate this, last June I was handing out diploma covers at graduation. As one of our well-known students (at least in the Financial Aid Office) stepped up to be introduced, she gave me a big hug and said thank-you. This is something I will always remember, because we don't always get a thank-you from one of our students. But they do appreciate what we do for them.

Remember this when you talk to that student for the 15th time or when you try to explain to another student why a .2 GPA isn't high enough for financial aid. Remember this when you are trying to calm down that angry parent who just doesn't understand why you denied Junior's appeal for independent status. Laugh about the funny situation and empathize with the sad situations. Call your peers in the state when you need help and offer your help to others. Always remember that you are helping others achieve their dreams!

News & Announcements

The polls are closed and the people have spoken. And the winner is . . . .

UASFAA President-elect – Terry Stevens, Davis UATC
Associate Member-elect – Michelle Riddle, UHEAA

A big Thank You to all who agreed to offer support by running for office and serving on committees.

Dr. Mark H. Spencer, Associate Commissioner
and Executive Director, UHEAA

Dr. Mark Spencer joined the Utah System of Higher Education in 2002 as associate commissioner for Finance and Facilities. In May, 2004, he was given an additional assignment as acting executive director of UHEAA (Utah Higher Education Assistance Authority). He was named executive director in December, 2004.

He came to the System Office from Utah Valley State College, where he had been CIO, associate vice president for Planning, and dean of General Studies. He worked previously at the College of Eastern Utah, Ohio State University, and University of Utah, and held adjunct faculty positions at the institutions listed above as well as Utah State University. His doctoral work at Ohio State University included studies in educational administration and public finance.

TERI NAMES NEW PRESIDENT

The Education Resources Institute, Inc. Names Willis J. Hulings III to Top Post

Contact: Marjorie Arons-Barron
Barron Associates Worldwide, Inc.
617-423-7770

Contact: Jane Dixon
TERI
(617) 556-0530

For immediate release

Boston, MA. January 18, 2005 –The Education Resources Institute, Inc. (TERI), has named Willis J. Hulings III to be President and Chief Executive Officer. He will join TERI in February. (Ronell, These folks need to check their caps – this is wrong, but you can't change it because it is in their official release ☺. You might want to invest in a copy of *The Chicago Manual of Style*. There is great info starting on p. 240.)

"We are delighted that Willis Hulings has agreed to join TERI and bring his vast financial expertise and leadership to the arena of higher education opportunity," said TERI Board Chair Dr. Sherry Penney. "His outstanding background and his deep commitment to TERI's mission make him uniquely suited to lead TERI at this time. We are very grateful to Larry O'Toole, TERI's current President and CEO, for showing great leadership over the last few years when the organization was at a critical turning point and bringing it to the success it is today."

Mr. Hulings has held senior management positions in financial services firms, including Capital One Financial Corporation, Wachovia Corporation, Kidder Peabody and Manufacturers Hanover Trust. He is

a graduate of Yale University and received his MBA from the Wharton School at the University of Pennsylvania.

TERI is the oldest and largest non-profit guarantor of private student loans, bringing together lenders, schools, students and families to make available low-cost, high-quality financing of postsecondary education with over $5 billion in outstanding loans under guarantee. TERI's College Access Division provides information and guidance to empower underserved students to achieve their educational goals, and it works to improve student achievement and teacher preparation in Boston. TERI College Access also plays a prominent national and regional leadership role in identifying and promoting strategies for improving college access and financial aid.

"This is an exciting and critical time in TERI's history, and I am enthusiastic about the opportunities and challenges facing TERI as it continues to experience tremendous growth," said Mr. Hulings. "I am pleased to be working with TERI College Access as it continues its creative outreach to new generations of college students and adult learners, bringing within their grasp the dream of higher education."

TERI has a highly successful strategic alliance with First Marblehead Corporation, through which annual loan volume has grown to over $2 billion. In his new role, Mr. Hulings will oversee that alliance to ensure TERI's continued position as a market leader in guaranteeing student loans.

TERI is a Boston, Massachusetts based non-profit organization founded in 1985. For additional information, visit TERI on the web at www.teri.org or call (800) 255-TERI.

Upcoming Events

UASFAA Spring Conference
Celebrate the Past, Build the Future

April 20, 21 & 22, 2005
St. George, UT

Please register and pay fees by April 5th.

The conference will be held at the Dixie Center

For lodging reservations call the Fairfield Inn. Mention UASFAA

US Department of Education Spring Conference – March 22-24, 2005 in Reno, NV. See http://www.ed.gov/offices/OSFAP/conferences/index.html for more information on this and the following EAC conferences.

Electronic Access Conference – October 30 to November 2, 2005, San Diego, CA
Electronic Access Conference – November 29 to December 2, 2005, Atlanta, GA

2005 UASFAA Conference – April 20-22 in St. George at the Dixie Center

Summer Institute – June 12-17, 2005, Colorado School of Mines

2005 NASFAA Conference – July 3-6, 2005, New York, NY

2005 RMASFAA Conference – October 9-12, 2005, Jackson Hole, WY

2006 US Department of Education Spring Conference – April 5-7, 2006 in San Antonio, TX

Electronic Access Conference, October 30 to November 2, 2006 in Orlando, FL
Electronic Access Conference, November 28 to December 1, 2006 in Las Vegas, NV

Spotlight

Brian McGill, Manager of Outreach Programs, UHEAA

Brian McGill was recently appointed manager of Outreach Services for UHEAA. Brian has been the senior outreach services officer for just over a year. He has been actively advancing UtahMentor, UHEAA's comprehensive college preparation web site, to middle and high school students throughout the state of Utah. Brian will continue to train middle & high school counselors, careers teachers, and other district leaders about financial aid, career and college opportunity learning for students and parents in using UtahMentor, and assisting school counselors with students' SEOP (Student Educational Occupational Plan) process by conducting student focus groups at various schools across Utah. Brian will also provide UtahMentor support to the Utah Council, PTSA, State Office of Education, and other state, national, and community organizations. Brian's vision for UtahMentor parallels a vision he had at Riverton High School by creating and programming a customized school counseling Web site in which students, parents, faculty, and counselors had access to state of the art career, college, financial aid, and scholarship information. What Brian terms, "An electronic one-stop shopping source for students and parents which provides access to post-secondary educational and occupational opportunities." Brian will continue with his vision using UtahMentor as this tool, and will look to continually improve and update the site to meet the needs of Utah students, parents and counselors.

Before coming to UHEAA Brian served as a high school counselor and tennis coach for both the boys and girls tennis programs at Riverton High School. Brian served on a committee in 2003 to critique and make changes to Utah's current model for the Comprehensive Guidance Counseling Performance Review, which all of Utah's middle and high schools have to go through every three years to comply with comprehensive guidance counseling. Riverton High School's Counseling Performance Review received very high reviews and now serves as the present state model available on the Utah State Office of Education's Web site at www.usoe.k12.ut.us/ate/compguide/review . Previously, Brian worked in the clinical counseling field and served as a middle school counselor at North Layton Junior High in Davis School District and Oquirrh Hills Middle School in Jordan School District. Brian has earned a combined masters degree in educational and clinical counseling from the University of Phoenix, is a licensed professional counselor, and has a bachelor's degree in psychology from the University of Utah.

Brian received the Educator of the Year award in the Jordan School District for the 2002-2003 school year. Last year he was selected as the Utah High School Tennis Coach of the Year through the National Foundation for High School Coaches.

Brian has presented and spoken at numerous educational and counseling conferences, including conferences sponsored by USOE, USCA, Utah Alliance for Concurrent Enrollment, UASFAA, UACRAO, and the Wasatch Front Counselors Conference. He also serves on the American Indian/Alaskan Native State Education Plan, a Federal AP Incentive Grant committed to provide funding for disadvantaged students, plus serves on committees for the Utah Council and the State Office of Ethnic Affairs, including recently having had the opportunity of presenting at the 2003 African-American and 2005 Hispanic GIFT (Governor's Initiative for Families Today) Conferences focused on youth.

Brian is the proud father of a two-year old daughter named Miken, and is approaching his 9th year of marriage with his wife Jody. Brian enjoys many interests and hobbies, including weight training, tennis,

traveling, and keeping actively involved regarding positive student outcomes and issues involving public and higher education. Brian was born and raised in Mesa, Arizona, moved to Sandy, Utah in 1985, and currently resides in Draper.

Movers & Shakers

Shannon Sheaff
Account Manager,
Bank One Education Finance Corporation

Bank One Education Finance Corporation is pleased to announce that Shannon Sheaff has joined its office as an account manager for Utah, Colorado and Wyoming. Shannon comes to Bank One with 13 years experience in the financial aid industry including stops at Stony Brook University, the University of Northern Colorado and the University of Wyoming. Shannon will be located in the Denver, Colorado office.

John Curl,
Director of Financial Aid
It took a while but the University of Utah finally chose John Curl to be the director of financial aid. Congratulations, John.

Brad Ewell has moved to U.S. Bank at the first of August 2004 as the new market manager for Utah, Arizona and Nevada. He most recently worked for nine years as the associate executive director for Loan Purchase Program (LPP) Oversight and Coordination for Utah Higher Education Assistance Authority (UHEAA). He worked in several positions while at UHEAA, including senior program operations officer, manager of Program Operations, director of Customer Service for LPP and associate executive director for LPP Oversight and Coordination. Brad began his banking career in 1984 with First Security Bank of Utah, and then went on to Zions Bank prior to his time with UHEAA. He has worked in student lending since 1988.

Brad and his wife of almost 18 years, Teri, have two daughters, Carly (13) and Bailie (10). Teri enjoys her position as a librarian at an elementary school. Carly and Bailie both play sports and the piano, and Carly has recently started learning the harp.

BYU Financial Aid Office
Andrea Beck, an admissions counselor, is also a financial aid counselor. In addition, the processors of both the Financial Aid and Admissions Offices are cross-training. Never a dull moment.

We have also created a Help Desk manned or if you prefer, “womaned” by **Kelly Wilson**, to assist other offices who have questions about their own or student interaction with the Financial Aid Office.

Vacation Destinations

Stan Roberts,
Mountain America

My favorite place is located in North County, San Diego. The town of Cardiff by the Sea - San Elijo State Beach.

We vacation on the 24th of July - an extra day off for most of our neighbors.
Reservations are accepted on January 2, 200x and it fills up before 9:30am

---

Cristi Easton,
Salt Lake Community College

Our family's favorite spot to go on vacation is right here in Utah. Each summer we spend a week at Fish Lake in central Utah. Fish Lake is a located on a national forest. If you haven't been there before, you're missing a beautiful spot. The lake is large and deep and there are cabins, camping areas, boats to rent and a clear sky that is full of stars on a summer evening. We have been going there for over 20 years (yes, I am that old!). Although I don't fish, I love just sitting on the boat enjoying the view and reading a good book. You have to go early enough in the season that the fishing is good, but not so early that you get snow. (We started staying in the cabins the year after I

had to knock ice off the tent!) One other tradition with this vacation is that we stop in Nephi at the "One Man Band Cafe." Their cream cheese omelet is to die for.

Karen Henriquez,
University of Utah

I have not had my most memorable vacation yet. It will be this summer after my husband returns from Afghanistan. We plan to go to Mexico and play.

Alayne Sutherland,
America First Credit Union

A couple of years ago we pulled our 21-foot boat up to the coast of Washington, put it and our truck on a ferry and went to the San Juan Islands. We spent about five days there whale watching, boating around the islands, catching and eating fresh crab and totally had a wonderful time.

Lynn Jensen,
BYU

No need to look further than Utah's Dixie, and I'm not just whistling the Cougar fight song either. It has everything anyone would want (except the surf).

Need To Know

ID Theft: What's It All About

Reprinted from the Federal Trade Commission's
Web site at: http://www.consumer.gov/idtheft/

Dear Consumer:

The Federal Trade Commission has published this booklet to help raise consumer awareness of identity theft.

If you or someone you know is a victim of identity theft, please visit www.consumer.gov/idtheft. The information you enter there becomes part of a secure database that's used by law enforcement officials across the nation to help stop identity thieves. The site also has links to useful information from other federal agencies, states and consumer organizations.

You also may want to call 1-877-ID THEFT, the

FTC's toll-free ID Theft Hotline, where counselors help consumers who want or need more information about dealing with the consequences of identity theft.

We encourage you to share this booklet with your family, friends, colleagues, and neighbors.

Sincerely,

Carolyn S. Shanoff, Associate Director
Consumer and Business Education
Bureau of Consumer Protection, Federal Trade Commission

Introduction

The 1990's spawned a new variety of crooks called identity thieves. Their stock in trade? Your everyday transactions, which usually reveal bits of your personal information: your bank and credit card account numbers; your income; your Social Security number (SSN); or your name, address, and phone numbers. An identity thief obtains some piece of your sensitive information and uses it without your knowledge to commit fraud or theft.

Identity theft is a serious crime. People whose identities have been stolen can spend months or years — and their hard-earned money — cleaning up the mess the thieves have made of their good name and credit record. Some victims have lost job opportunities, been refused loans for education, housing or cars, or even been arrested for crimes they didn't commit.

Can you prevent identity theft from occurring? As with any crime, you cannot completely control whether you will become a victim. But, according to the Federal Trade Commission (FTC), you can minimize your risk by managing your personal information cautiously and with heightened sensitivity.

How Identity Theft Occurs

Skilled identity thieves use a variety of methods to gain access to your personal information. For example:

- They get information from businesses or other institutions by:
  - stealing records from their employer,
  - bribing an employee who has access to these records, or
  - hacking into the organization's computers.
- They rummage through your trash, or the trash of businesses or dumps in a practice known as "dumpster diving."
- They obtain credit reports by abusing their employer's authorized access to credit reports or by posing as a landlord, employer, or someone else who may have a legal right to the information.
- They steal credit and debit card numbers as your card is processed by using a special information storage device in a practice known as "skimming."
- They steal wallets and purses containing identification and credit and bank cards.
- They steal mail, including bank and credit card statements, pre-approved credit offers, new checks, or tax information.
- They complete a "change of address form" to divert your mail to another location.
- They steal personal information from your home.
- They scam information from you by posing as a legitimate business person or government official.

Once identity thieves have your personal information, they may:

- Go on spending sprees using your credit and debit card account numbers to buy “big-ticket” items like computers that they can easily sell.
- Open a new credit card account, using your name, date of birth, and SSN. When they don’t pay the bills, the delinquent account is reported on your credit report.
- Change the mailing address on your credit card account. The imposter then runs up charges on the account. Because the bills are being sent to the new address, it may take some time before you realize there’s a problem.
- Take out auto loans in your name.
- Establish phone or wireless service in your name.
- Counterfeit checks or debit cards, and drain your bank account.
- Open a bank account in your name and write bad checks on that account.
- File for bankruptcy under your name to avoid paying debts they’ve incurred, or to avoid eviction.
- Give your name to the police during an arrest. If they are released and don’t show up for their court date, an arrest warrant could be issued in your name.

How Can I Tell if I’m a Victim of Identity Theft?

Monitor the balances of your financial accounts. Look for unexplained charges or withdrawals. Other indications of identity theft can be:

- failing to receive bills or other mail signaling an address change by the identity thief;
- receiving credit cards for which you did not apply;
- denial of credit for no apparent reason; or
- receiving calls from debt collectors or companies about merchandise or services you didn’t buy.

Are There Any Other Steps I Can Take?

If an identity thief is opening new credit accounts in your name, these accounts are likely to show up on your credit report. You can find out by ordering a copy of your credit report from any of three major credit bureaus. If you find inaccurate information, check your reports from the other two credit bureaus. Of course, some inaccuracies on your credit reports may be because of computer, clerical, or other errors and may not be a result of identity theft. Note: If your personal information has been lost or stolen, you may want to check all of your reports more frequently for the first year. Federal law allows credit bureaus to charge you up to $9 for a copy of your credit report. Some states may allow a free report or reduced rates.

Managing Your Personal Information

So how can a responsible consumer minimize the risk of identity theft, as well as the potential for damage? When it involves your personal information, exercise caution and prudence.

Do It Now

Place passwords on your credit card, bank and phone accounts. Avoid using easily available information like your mother’s maiden name, your birth date, the last four digits of your SSN or your phone number, or a series of consecutive numbers. When you’re asked for your mother’s maiden name on an application for a new account, try using a password instead.

Secure personal information in your home, especially if you have roommates, employ outside help, or are having service work done in your home.

Ask about information security procedures in your workplace. Find out who has access to your personal information and verify that your records are kept in a secure location. Ask about the disposal procedures for those records as well.

Everyday Diligence

Don't give out personal information on the phone, through the mail, or over the Internet unless you've initiated the contact or are sure you know who you're dealing with. Identity thieves can be skilled liars, and may pose as representatives of banks, Internet service providers (ISPs), or even government agencies to get you to reveal identifying information. Before you divulge any personal information, confirm that you're dealing with a legitimate representative of a legitimate organization. Double check by calling customer service using the number on your account statement or in the telephone book.

Guard your mail and trash from theft. Deposit outgoing mail in post office collection boxes or at your local post office instead of an unsecured mailbox. Remove mail from your mailbox promptly. If you're planning to be away from home and can't pick up your mail, call the U.S. Postal Service at 1-800-275-8777 to ask for a vacation hold. To thwart a thief who may pick through your trash or recycling bins, tear or shred your charge receipts, copies of credit applications or offers, insurance forms, physician statements, checks and bank statements, and expired charge cards.

Before revealing any identifying information (for example, on an application), ask how it will be used and secured, and whether it will be shared with others. Find out if you have a say about the use of your information. For example, can you choose to have it kept confidential?

Keep your Social Security card in a secure place and give your SSN only when absolutely necessary. Ask to use other types of identifiers when possible. If your state uses your SSN as your driver's license number, ask to substitute another number.

Limit the identification information and the number of credit and debit cards that you carry to what you'll actually need.

Keep your purse or wallet in a safe place at work.

Consider Your Computer

Your computer can be a goldmine of personal information to an identity thief. Here's how you can safeguard your computer and the personal information it stores:

- Update your virus protection software regularly. Computer viruses can have damaging effects, including introducing program code that causes your computer to send out files or other stored information. Look for security repairs and patches you can download from your operating system's Web site.
- Don't download files from strangers or click on hyperlinks from people you don't know. Opening a file could expose your system to a computer virus or a program that could hijack your modem.
- Use a firewall, especially if you have a high-speed or "always on" connection to the Internet. The firewall allows you to limit uninvited access to your computer. Without a firewall, hackers can take over your computer and access sensitive information.
- Use a secure browser — software that encrypts or scrambles information you send over the Internet — to guard the safety of your online transactions. When you're submitting information, look for the "lock" icon on the status bar. It's a symbol that your information is secure during transmission.
- Try not to store financial information on your laptop unless absolutely necessary. If you do, use a "strong" password — that is, a combination of letters (upper and lower case), numbers, and symbols.
- Avoid using an automatic log-in feature that saves your user name and password; and always log off when you're finished. If your laptop gets stolen, the thief will have a hard time accessing sensitive information.

- Delete any personal information stored on your computer before you dispose of it. Use a “wipe” utility program, which overwrites the entire hard drive and makes the files unrecoverable.
- Read Web site privacy policies. They should answer questions about the access to and accuracy, security, and control of personal information the site collects, as well as how sensitive information will be used, and whether it will be provided to third parties.

A Special Word About Social Security Numbers

Very likely, your employer and financial institution will need your SSN for wage and tax reporting purposes. Other private businesses may ask you for your SSN to do a credit check, such as when you apply for a car loan. Sometimes, however, they simply want your SSN for general record keeping. If someone asks for your SSN, ask the following questions:

- Why do you need it?
- How will it be used?
- How do you protect it from being stolen?
- What will happen if I don’t give it to you?

If you don’t provide your SSN, some businesses may not provide you with the service or benefit you want. Getting satisfactory answers to your questions will help you to decide whether you want to share your SSN with the business.

If Your Identity’s Been Stolen

Even if you’ve been very careful about keeping your personal information to yourself, an identity thief can strike. If you suspect that your personal information has been used to commit fraud or theft, **take the following four steps right away**. Remember to follow up all calls in writing; send your letter by certified mail, return receipt requested, so you can document what the company received and when; and keep copies for your files.

1. Place a fraud alert on your credit reports and review your credit reports.

Call the toll-free fraud number of anyone of the three major credit bureaus to place a fraud alert on your credit report. This can help prevent an identity thief from opening additional accounts in your name. As soon as the credit bureau confirms your fraud alert, the other two credit bureaus will automatically be notified to place fraud alerts on your credit report, and all three reports will be sent to you free of charge.

- **Equifax** — To report fraud, call:
  1-800-525-6285, and write: P.O. Box 740241, Atlanta, GA 30374-0241
- **Experian** — To report fraud, call:
  1-888-EXPERIAN (397-3742), and write: P.O. Box 9532, Allen, TX 75013
- **TransUnion** — To report fraud, call:
  1-800-680-7289, and write: Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790

Once you receive your reports, review them carefully. Look for inquiries you didn’t initiate, accounts you didn’t open, and unexplained debts on your true accounts. You also should check that information such as your SSN, address(es), name or initial, and employers are correct. Inaccuracies in this information also may be due to typographical errors. Nevertheless, whether the inaccuracies are due to fraud or error, you should notify the credit bureau as soon as possible by telephone and in writing. You should continue to check your reports periodically, especially in the first year after you’ve discovered the theft, to make sure no new fraudulent activity has occurred. The automated “one-call” fraud alert process only

works for the initial placement of your fraud alert. Orders for additional credit reports or renewals of your fraud alerts must be made separately at each of the three major credit bureaus.

2. Close any accounts that have been tampered with or opened fraudulently.

Credit Accounts

Credit accounts include all accounts with banks, credit card companies and other lenders, and phone companies, utilities, ISPs, and other service providers.

If you're closing existing accounts and opening new ones, use new Personal Identification Numbers (PINs) and passwords.

If there are fraudulent charges or debits, ask the company about the following forms for disputing those transactions:

- For new unauthorized accounts, ask if the company accepts the ID Theft Affidavit (available at www.ftc.gov/bcp/conline/pubs/credit/affidavit.pdf). If they don't, ask the representative to send you the company's fraud dispute forms.
- For your existing accounts, ask the representative to send you the company's fraud dispute forms.
- If your ATM card has been lost, stolen or otherwise compromised, cancel the card as soon as you can. Get a new card with a new PIN.

Checks

If your checks have been stolen or misused, close the account and ask your bank to notify the appropriate check verification service. While no federal law limits your losses if someone steals your checks and forges your signature, state laws may protect you. Most states hold the bank responsible for losses from a forged check, but they also require you to take reasonable care of your account. For example, you may be held responsible for the forgery if you fail to notify the bank in a timely way that a check was lost or stolen. Contact your state banking or consumer protection agency for more information.

You also should contact these major check verification companies. Ask that retailers who use their databases not accept your checks.

TeleCheck — 1-800-710-9898 or 927-0188

Certegy, Inc. — 1-800-437-5120

International Check Services — 1-800-631-9656

Call SCAN (1-800-262-7771) to find out if the identity thief has been passing bad checks in your name.

3. File a report with your local police or the police in the community where the identity theft took place.

Keep a copy of the report. You may need it to validate your claims to creditors. If you can't get a copy, at least get the report number.

4. File a complaint with the FTC.

By sharing your identity theft complaint with the FTC, you will provide important information that can help

law enforcement officials track down identity thieves and stop them. The FTC also can refer victim complaints to other appropriate government agencies and companies for further action. The FTC enters the information you provide into our secure database.

To file a complaint or to learn more about the FTC's Privacy Policy, visit www.consumer.gov/idtheft. If you don't have access to the Internet, you can call the FTC's Identity Theft Hotline: toll-free 1-877-IDTHEFT (438-4338); TDD: 202-326-2502; or write: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

The FTC works for the consumer to prevent fraudulent, deceptive and unfair business practices in the marketplace and to provide information to help consumers spot, stop, and avoid them. To file a complaint or to get free information on consumer issues, visit www.ftc.gov or call toll-free, 1-877-FTC-HELP (1-877-382-4357); TTY: 1-866-653-4261. The FTC enters Internet, telemarketing, identity theft, and other fraud-related complaints into Consumer Sentinel, a secure, online database available to hundreds of civil and criminal law enforcement agencies in the U.S. and abroad.

October 2003

Editor's Note
Other good information on preventing identity theft written by Robert Sherman can be found at http://www.identity-theft-help.us/identity-theft-prevention.htm

Here are recent examples of credit card fraud I received in an e-mail this month. What's in your wallet?

CREDIT CARDS SCENE 1

A friend went to the local gym and placed his belongings in the locker. After the workout and a shower, he came out, saw the locker open, and thought to himself, "Funny, I thought I locked the locker. Hmmmmm." He dressed and just flipped the wallet to make sure all was in order.

Everything looked okay - all cards were in place. A few weeks later his credit card bill came - a whooping bill of $14,000! He called the credit card company and started yelling at them, saying that he did not make the transactions. Customer care personnel verified that there was no mistake in the system and asked if his card had been stolen card, and yep - you guessed it - a switch had been made. An expired similar credit card from the same bank was in the wallet. The thief broke into his locker at the gym and switched cards.

Verdict: The credit card issuer said since he did not report the card missing earlier, he would have to pay the amount owed to them. How much did he have to pay for items he did not buy? $9,000! Why were there no calls made to verify the amount swiped? Small amounts rarely trigger a "warning bell" with some credit card companies. It just so happens that all the small amounts added up to big one!

SCENE 2

A man at a local restaurant paid for his meal with his credit card. The bill for the meal came, he signed it, and the waitress folded the receipt and passed the credit card along. Usually, he would just take it and place it in his wallet or pocket. Funny enough, though, he actually took a look at the card and, lo and behold, it was the expired card of another person.

He called the waitress and she looked perplexed. She took it back, apologized, and hurried back to the counter under the watchful eye of the man. All the waitress did while walking to the counter was wave the wrong expired card to the counter cashier, and the counter cashier immediately looked down and took out the real card. No exchange of words --- nothing! She took it and came back to the man with an

apology.

Verdict: Make sure the credit cards in your wallet at yours. Check the name on the card every time you sign for something and/or the card is taken away for even a short period of time. Many people just take back the credit card without even looking at it, thinking that it has to be theirs.

FOR YOUR OWN SAKE, DEVELOP THE HABIT OF CHECKING YOUR CREDIT CARD EACH TIME IT IS RETURNED TO YOU AFTER A TRANSACTION!

SCENE 3

Yesterday I went into a pizza restaurant to pick up an order that I had called in. I paid by using my Visa Check Card which, of course, is linked directly to my checking account. The young man behind the counter took my card, swiped it, then laid it flat on the counter as he waited for the approval, which is pretty standard procedure.

While he waited, he picked up his cell phone and started dialing. I noticed the phone because it is the same model I have, but nothing seemed out of the ordinary. Then I heard a click that sounded like my phone sounds when I take a picture. He then gave me back my card but kept the phone in his hand as if he was still pressing buttons.

Meanwhile, I'm thinking: I wonder what he is taking a picture of, oblivious to what was really going on. It then dawned on me: the only thing there was my credit card, so now I'm paying close attention to what he is doing.

He set his phone on the counter, leaving it open. About five seconds later, I heard the chime that tells you that the picture has been saved. Now I'm standing there struggling with the fact that this boy just took a picture of my credit card. Yes, he played it off well, because had we not had the same kind of phone, I probably would never have known what happened.

Needless to say, I immediately canceled that card as I was walking out of the pizza parlor. All I am saying is, be aware of your surroundings at all times. Whenever you are using your credit cards, take caution and don't be careless. Notice who is standing near you and what they are doing when you use your card. Be aware of phones because many have a camera phone these days.

When you are in a restaurant and the waiter/waitress brings your card and receipt for you to sign, make sure you scratch the number off. Some restaurants are using only the last four digits, but a lot of them are still putting the whole thing on there. I have already been a victim of credit card fraud and, believe me, it is not fun. The truth is that they can get you even when you are careful, but don't make it easy for them.