

# Fraud Prevention and Consumer Protection

Presented by

Melanie D. Jewkes, M.S.

USU Extension Assistant Professor

Family and Consumer Sciences

Duchesne County

**UtahState**  
UNIVERSITY

COOPERATIVE  
**extension**

# New Credit Card Scam

- The scam works like this: Caller: 'This is (name), and I'm calling from the Security and Fraud Department at VISA. My Badge number is 12460. Your card has been flagged for an unusual purchase pattern, and I'm calling to verify. This would be on your VISA card which was issued by (name of bank). Did you purchase an Anti-Telemarketing Device for \$497.99 from a Marketing company based in Arizona ?'
- When you say 'No' the caller continues with, 'Then we will be issuing a credit to your account. This is a company we have been watching and the charges range from \$297 to \$497, just under the \$500 purchase pattern that flags most cards. Before your next statement, the credit will be sent to (gives you your address), is that correct?'
- You say 'yes'. The caller continues - 'I will be starting a Fraud investigation. If you have any questions, you should call the 1- 800 number listed on the back of your card and ask for Security.'
- You will need to refer to this Control Number. The caller then gives you a 6 digit number. 'Do you need me to read it again?'

## Credit Card Scam 2

- The caller then says, 'I need to verify you are in possession of your card'. He'll ask you to 'turn your card over and look for some numbers'. There are 7 numbers; the first 4 are part of your card number, the next 3 are the security Numbers that verify you are the possessor of the card. These are the numbers you sometimes use to make Internet purchases to prove you have the card.
- The caller will ask you to read the 3 numbers to him. After you tell the caller the 3 numbers, he'll say, 'That is correct, I just needed to verify that the card has not been lost or stolen, and that you still have your card. Do you have any other questions?' After you say No, the caller then thanks you and states, 'Don't hesitate to call back if you do, and hangs up.'

## Credit Card Scam 3

- You actually say very little, and they never ask for or tell you the Card number.
- But after we were called on Wednesday, we called back within 20 minutes to ask a question. Are we glad we did! The REAL VISA Security Department told us it was a scam and in the last 15 minutes a new purchase of \$497.99 was charged to our card.
- What the scammers want is the 3-digit PIN number on the back of the card Don't give it to them. Instead, tell them you'll call VISA or Master card directly for verification of their conversation.

# Ogden couple falls victim to scam

- Friday, August 29, 2008 by **SAM COOPER** Standard-Examiner staff
- Ogden couple falls victim to scam August 29th, 2008 @ 1:24pm By Becky Bruce
- When the phone rang in the middle of the night, Vernon and Alice Harper knew something was wrong.
- Alice said the caller told her, "Oh, I'm sorry, Grandma. I'm really sorry to do this to you." She said it sounded a little bit like he was crying. The caller told them, "I'm in trouble, Grandma. I'm up here in Toronto. I need money. I'm in jail. I had a rented car, and I wrecked it."
- They thought the caller was their grandson, so Alice wired \$4,400. The caller said his calling card only had a few minutes and he didn't have much time, but could she wire the money within two hours? He would call back in two hours to get the personal identification number.

## Ogden couple falls victim to scam 2

- The convincing "grandson" said he'd gone to Canada the night before and couldn't talk long because he was using a calling card that was running out of minutes.
- "He said he had the money -- I knew he did -- and he'd pay it back," Alice Harper said.
- The caller talked the couple into sending him a \$4,400 MoneyGram from the Wal-Mart in Harrisville so he could get out of jail.
- "They do appeal to you," Alice Harper said. "He said, 'Grandma, I love you,' and, 'I'm sorry I did this.' "
- When she called her grandson the next day to make sure everything was OK, he didn't know what she was talking about. Alice said, "I called him and I said, 'What time did you get home last night?' And he said, 'Get home from where?'"

## Comment on *Standard Examiner*

- “This happened to me also in TX. “He sounded so real.” As I was ready to write down directions to send money...I asked for one more thing..."tell me something that only you & I would know so that I KNOW you're who you are." The caller hung up. I reported story to our Police Dept.”

# Provo police cracking down on asphalt scam

- August 29th, 2008 @ 4:50pm By Randall Jeppesen
- Provo police are trying to track down pavers **who are scamming the elderly** out of thousands of dollars.
- Police have two cases so far, but believe there are many more victims.
- Helen Anderson, spokeswoman for the Provo Police Department, said, "They seem to be **focusing on the elderly or vulnerable people**. They knock on the door and say, 'Hey, we're a business that does asphalt. We noticed that you might need some. We have some extra black top in the back of our truck.'"
- The problem, Anderson said, is they will do much more work than is authorized. She said, "They use a lot more black top from their truck, and then they charge for the entire amount. And people are complaining that they've **been charged instead of say \$1,700, they are being charged \$8,000.**"
- Anderson said the scammers even followed the homeowners to the bank to make sure they got paid.
- Police believed one group running the scam has already left town, but they thought there were others in the area.
- **Anderson said if your are going to have work done on your home, make sure you get the price in writing.**

## Comment on KSL

- “like PT BARNUM SAID, a sucker is born every second, SO DONT BE ONE, JUST USE COMMON SENSE and don't be SO TRUSTING, crooks profit off your misplaced trust then laugh at you.”



# Identity Theft

- Take ID Theft quiz
- What does this tell us about preventing ID Theft?
- In addition, consider these tips:
  - Pay attention to your billing cycles
  - Be proactive at work
    - Who has access to your personal records?
      - Are those records kept secure and shredded?



# Preventing ID Theft

- Tips for Checkbook:
  - Don't write full account numbers on checks to pay credit card bills. Just write the last 4 digits.
  - Print only first initial on checks
    - Example: A. Johnson (not Adam Johnson)
      - If checkbook is stolen, thieves won't know whether you sign your checks with initials, first name or a shortened name. Your bank will know how you sign your checks and will pull suspicious checks and call to verify the purchase.



# Preventing ID Theft



- **Wallet Tips:**
  - Watch credit cards closely. Thieves are getting more creative with the use of cell phone cameras, etc.
  - Copy contents of wallet (front and back sides)
    - Place this in a safe, convenient location
    - When wallet is missing or stolen, immediately call the credit card companies, insurance companies, banks, etc.

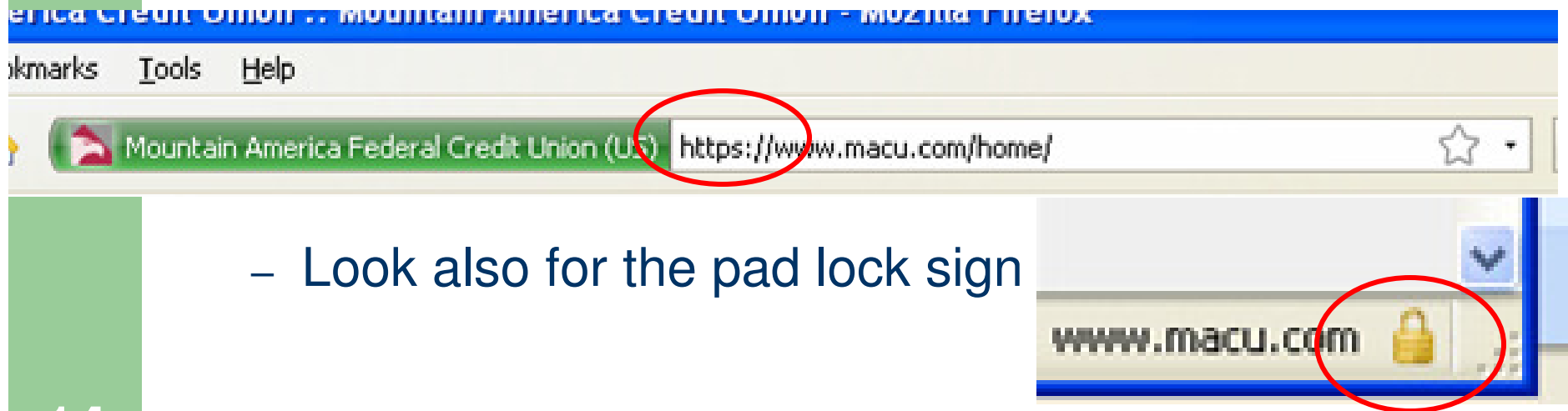
# Preventing ID Theft

- Password Tips:
  - Guard passwords. Don't carry with you.
    - Top 10 Most Commonly used passwords (in mid 2007)
      1. password
      2. 123456
      3. Qwerty
      4. abc123
      5. Letmein
      6. Monkey
      7. myspace1
      8. password1
      9. blink182
      10. (your first name)



# Preventing ID Theft

- Internet Tips:
  - Look for “https://” before entering social security number, credit card numbers, account numbers, etc.



- Look also for the pad lock sign

# Warning Signs of Fraudulent or Deceptive Schemes

- Ask for your personal information
  - Social security number
  - Account numbers
  - Passwords
  - Credit card number
  - Birthdates
  - Verification numbers on back of credit cards
- Sense of urgency
- Guaranteed profit, little risk
  - If it sounds too good to be true...
- Relationships of trust (“just trust me”)
- Well-known referrals (if so-and-so has done this, it must be good)



# Top 10 Consumer Scams E-Commerce/Internet Offers

- Old scams are being repackaged with the new forms of electronic communication through emails and the Internet. Some common deceptive e-commerce practices are:
  - Products are advertised as “FREE” when there are undisclosed hidden fees;
  - Consumers’ bank accounts are automatically charged according to the company’s hidden terms until the consumer gives notice of cancellation (“negative option”);
  - Consumer’s right to cancel is not clearly stated; and
  - Contains false testimonials and other misrepresentations.

# Top 10 Consumer Scams

## Auto Repair

- Repair shops commit deceptive practices when they:
  - fail to obtain the consumer's authorization before performing repairs;
  - Perform unneeded repairs;
  - Fail to honor their warranties;
  - Misrepresent their products/services; and
  - Fail to disclose refund policies.

# Top 10 Consumer Scams

## Home Based Business Opportunities

- Consumers buy into the “get rich quick” schemes of owning their own home-based business. Their purchase usually leads to the purchase of additional services such as a mentoring or coaching program. The cost of the additional services usually involves large sums of money. Some of the problems are that the seller of the business opportunity:
  - Does not provide the disclosures as required by the Business Opportunity Disclosure Act;
  - Engages in deceptive business practices in violation of the Utah Consumer Sales Practices Act (ie. Fails to give right to cancel or to disclose refund policies);
  - Fails to deliver what was promised.



# Top 10 Consumer Scams

## Prizes/Sweepstakes

- These are old scams that take advantage of the Internet and electronic banking. The typical scam works this way:
  - Consumer receives notice of winning a large sum of money.
  - The notice explains the recipient's obligations to pay certain costs and gives a telephone number to call to claim the "winnings."
  - A check made out to the consumer for around \$5,000.00 is usually included with the notice.
  - When the telephone number is called the consumer is instructed to deposit the check and after it clears to wire a portion of that amount back via money gram or Western Union.
  - The check is later determined to be a forgery and must be refunded by the consumer.
  - Identity theft is usually involved.

# Top 10 Consumer Scams

## Mail Order & Contractor Fraud

- Mail Order
  - Each year more catalogues find their way into our homes. Although most mail order companies are legitimate, some are not. The consumer needs to take precautions to know who is being dealt with
- Contractor Fraud
  - When the weather improves, scams often involve home repairs or improvements. The typical scam is where the contractor accepts the homeowner's deposit and then fails to perform the services.

# Top 10 Consumer Scams

## Advance Fee Loans & Charity Donation Scams

- **Advance Fee Loans**

- The typical advance fee loan scam involves an advertisement for a loan to be provided regardless of the credit worthiness of the borrower. The borrower is required to pay an up-front fee. After paying this fee, the loan will be denied or the “lender” may request additional money to increase the amount applied for and then deny the loan.

- **Charity Donation Scams**

- Scam artists are always looking for new ways to take advantage of the public’s good will.

# Top 10 Consumer Scams

## Do-Not-Call & Collection Fraud

- **Do-Not-Call**

- The problem of telephone solicitations has dropped significantly in recent years largely because of the FTC's "Do Not Call" list that came into effect nearly 5 years ago. Unsolicited facsimiles continue to be a problem, but the new trend is to send unsolicited emails.

- **Collection Fraud**

- Some of the problems are
  - Interest charges;
  - Billing for unauthorized services; and
  - Deceptive practices of collection companies.

# Reducing Risk Check Credit Report



- Free credit report (from each of the 3 bureaus) per 12 months
- [www.annualcreditreport.com](http://www.annualcreditreport.com)
- To request credit report by phone:
  - Call 1-877-322-8228
  - you will go through a simple verification process over the phone.
  - Your reports will be mailed to you within 15 days. Please, allow 2-3 weeks for delivery.
- To Request your Credit Report by Mail:
  - Download the [request form](#) (*You need an Adobe viewer to view the requested form. [Download the free Adobe viewer](#)*)
  - Print and complete the form
  - Mail the completed form to:  
**Annual Credit Report Request Service**  
**P.O. Box 105281**  
**Atlanta, GA 30348-5281**
  - *Your reports will be mailed to you within 15 days. Please, allow 2-3 weeks for delivery.*

# Reducing Risk

## Fraud Alert on Credit Report

- **What is a Fraud Alert?**

A fraud alert is something that the major credit bureaus attach to your credit report. When you, or someone else, tries to open up a credit account by getting a new credit card, car loan, cell phone, etc., the lender should contact you by phone to verify that you really want to open a new account. If you aren't reachable by phone, the credit account shouldn't be opened.

- A creditor isn't required by law to contact you, however, even if you have fraud alert in place.
- The fraud alert will remain in place for only 90 days. When the time runs out, you'll need to reactivate the alert
- To do so, contact bureaus; ask them to place a fraud alert on your credit report

# Reducing Risk

## Freeze Credit Report

- Stronger than Fraud Alert
- If you are a victim of ID theft, or believe you are at increased risk, a security freeze can provide protection and peace of mind
- Security freeze prevents anyone from opening new credit accounts in your name
- Credit requests will likely be denied (even if you are asking for the credit)
- May cost money
- Equifax: 888-298-0045; [www.equifax.com](http://www.equifax.com)
- Experian: 888-397-3742;  
[www.experian.com/consumer/security\\_freeze.html](http://www.experian.com/consumer/security_freeze.html)
- TransUnion: 888-909-8872; [www.transunion.com](http://www.transunion.com)

# Reducing Risk

## Take Number Off Telemarketing Lists

- To **reduce unwanted phone solicitations**, send your name, address and telephone number, including area code, to:
  - TELEPHONE PREFERENCE SERVICE  
ATTN: Dept 10245520  
DIRECT MARKETING ASSOCIATION  
P.O. BOX 282  
CARMEL NY 10512
- **AND**, list number through the National Do Not Call Registry
  - Do not call registry: <http://www.donotcall.gov>
    - Or call: 1-888-382-1222 (TTY 1-866-290-4236) from the number you wish to register

# Reducing Risk

## Remove Name from Junk Mail Lists

- To **reduce unwanted junk mail**, send your name, address and telephone number, including area code, to:
  - MAIL PREFERENCE SERVICE  
ATTN: DEPT: 10245470  
DIRECT MARKETING ASSOCIATION  
P.O. BOX 282  
CARMEL NY 10512
  - You can also try to visit the following websites:
    - [www.junkbusters.com](http://www.junkbusters.com)
    - [www.catalogchoice.org](http://www.catalogchoice.org)
    - [www.41pounds.org](http://www.41pounds.org) (fee-based non-profit)
    - [www.greendimes.com](http://www.greendimes.com) (fee-based for-profit)



# Reducing Risk

## Remove Name from Unwanted Credit Solicitations

- To **reduce unwanted credit solicitations** (FOREVER, if you select the right option) go to:
- <http://www.Optoutprescreen.com>
  - make sure to select the permanent option, print pages, sign, and then mail in to provided address
- Or Call toll-free 1-888-5-OPTOUT (1-888-567-8688)
  - This will likely not be permanent—must mail in the “formal letter” to make permanent

## Reducing Risk Unwanted E-mail

- Don't open emails you don't recognize the sender. Send straight to spam folder.
- Opt-Out of the Direct Marketing Association's emailing list
  - visit [www.dmachoice.org/EMPS](http://www.dmachoice.org/EMPS). Your online request will be effective for five years.
  - Only stop those emails from companies subscribed to DMA
- If you get spam email that you think is deceptive, forward it to [spam@uce.gov](mailto:spam@uce.gov)
  - The FTC uses the spam stored in this database to pursue law enforcement actions against people who send deceptive email.

# Caveat Emptor

- *Caveat emptor*—let the buyer beware
- Used as a warning to anyone buying something that there might be unforeseen problems or faults with what is bought.
- Be an educated, careful consumer.
- Ask questions.
- Be skeptical.
- Follow your gut instinct.



# Filing a Complaint

- The Federal Trade Commission 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 [ftc.gov](http://ftc.gov) or <https://www.ftccomplaintassistant.gov/>
  - or call toll-free, 1-877-FTC-HELP (1-877-382-4357); TTY: 1-866-653-4261.
  - The FTC enters consumer complaints into the Consumer Sentinel Network, a secure online database and investigative tool used by hundreds of civil and criminal law enforcement agencies in the U.S. and abroad.

# If You Become a Victim of ID Theft

- **Do the following:**
- File a police report with the local law enforcement agency where the crime occurred or with the police or sheriff's office where you reside.
  - If the agency refers you to our office to file the report or tells you that they don't take those cases, you may need to respectfully request to speak with a supervisor who will take the report.
  - **Remember, if you are the victim of identity fraud, you are the victim of a crime!**
- Notify creditors, in writing, of the fraud. They may require you to sign a fraud affidavit or provide a police case number.
- Notify credit reporting agencies of the fraud. You should review your credit report for fraudulent entries so that you may challenge them and have the entries removed from the report.

# Victim of ID Theft:

- Cancel any accounts that suspects may have access to or change the account numbers. Be certain that your financial institutions are aware that you may be a victim of identity fraud so that they may take appropriate action to prevent additional crimes from being committed.
- Report the theft to the Federal Trade Commission at <http://www.ftc.gov>
- Report the theft to the Utah Attorney General's Office at <http://attorneygeneral.utah.gov> if you are a Utah resident.
- **Be patient!** Identity fraud crimes are generally quite complex and require extensive time and resources to solve.

# Sources

- Utah Division of Consumer Protection--  
<http://www.consumerprotection.utah.gov/>
- Federal Trade Commission--[ftc.gov](http://ftc.gov)
- KSL—[ksl.com](http://ksl.com)
- <http://www.standard.net/live/news/141883/>
- Jensen, C. (2008). Keep your identity safe.  
<http://extension.usu.edu/htm/news/articleID=3613>
- <http://www.threadwatch.org/node/14095>
- <http://www.fightidentitytheft.com/credit-freeze-laws.html>
- Wikitionary.com

**UtahState**  
UNIVERSITY

COOPERATIVE  
**extension**

Melanie D. Jewkes

PO Box 978

Duchesne, UT 84021

[melanie.jewkes@usu.edu](mailto:melanie.jewkes@usu.edu)

[extension.usu.edu/duchesne](http://extension.usu.edu/duchesne)

Office: (435) 738-1140

*“Utah State University is an Affirmative Action/Equal Opportunity Institution.”*