

# Identity Theft: *Who's Got Your Number?*



Brought to you by:  
Hughes Federal Credit Union



**Hughes**  
Federal Credit Union

*Yours for the asking™*



AMERICA'S  
CREDIT UNIONS™

## **Making a Positive Difference in Your Financial Life-**

- Credit unions are member-owned, democratically-run financial cooperatives.
- Member and community education is our ongoing mission.
- We reach out to our members; offering education online or in the community.
- We have 8 branches to serve you.  
Call us!
- 520-794-5341 or 800-253-8245

## **Online Seminar Objectives...**

### **Learn:**

- What identity theft is-
- How crooks get your personal information-
- When you have to give SSN, and when to say “no”-
- How to minimize risk of ID theft—online and offline-
- Tips to protect yourself from ‘phishing’ attacks-
- Warning signs that you may be a victim of ID theft-
- What to do if you’re a victim and where to get help-

## **What is Identity Theft?**

It occurs when someone uses your:

- Name
- Social Security number
- Credit card number
- Other identifying information...without your permission, to commit fraud or other crimes.

...without your permission,  
to commit fraud or other crimes.

## **Statistics on Victims**

Almost 10 million Americans (4.6% of the population) discovered they were the victim of some form of ID theft in the year before Sept. 2003.

(FTC Identity Theft Survey Report, Sept. 2003)

The State of Arizona ranks #1 in the U.S. for crimes related to ID Theft.

## **Impact on Victims**

Damaged credit record

Loss of job opportunities

Refused loans for education, housing, or cars

Spend months or years cleaning up the mess

Estimates:

- \$500 on average to deal with ID theft experience
- 300 hours resolving problems

Worst-case scenario:

Victim is arrested because of thief's criminal record

## **Who's Most Vulnerable?**

- People who don't take precautions
- People who are "out and about" using credit cards or debit cards, leaving receipts
- People who give personal information without asking "Why do you need it?"

## **How do Crooks get your Number?**

- Steal records from employer; computer hacking
- Steal wallet/purse
- Steal mail from unlocked mailbox statements, pre-approved credit offers, new checks, tax information
- Dumpster-diving for receipts, credit slips, applications
- Shoulder-surfing at ATMs or phone booths
- Pose as landlord or employer to obtain credit reports
- Fill out change of address form to divert your mail
- 'Phishing' via the Internet

## **Friendly Fraud... You Know the Thief**

- Safeguard your wallets, purses, checkbooks, and account statements—even in your home or at work
- Don't leave wallets in clear view of anyone coming into your home or office
- Review statements monthly for all charges, or more often online
- Don't write passwords or PINs on the back of the card or carry that information in your wallet
- For online transactions, use Verified by Visa and/or MasterCard's Secure Code
- Shred receipts, statements, and cancelled checks before discarding

## Beware "Skimming"

- The thief swipes your card through a hand-held device or overlay swipe device on an ATM
- The device gleans information (name, account number, expiration date, and security features) off magnetic stripe on the back of the card
- The thief copies the security codes from your card to the fraudulent card and sells it to a counterfeiter

TIPS: Review card statements, and use credit union- issued cards that have other security features. Look for an irregular type of device that may have been added to ATMs.

## **What do Crooks do with your Personal Information?**

- Go on spending sprees with your credit and debit account numbers
- Change mailing address on your credit card accounts; ring up charges before you realize it
- Take out loans in your name
- Establish phone service in your name
- File for bankruptcy in your name to avoid paying debts
- Give your name during an arrest

## **Tips to protect your SSN**

- Never give SSN, account numbers, passwords, mother's maiden name, birth date, PIN, or personal information over the phone, unless you initiated the call
- Keep SSN off driver's license
- Don't carry Social Security card in wallet unless you need it that day
- Don't use last 4 digits of SSN as PIN. Memorize PINs! Random issue PIN numbers are best.
- Don't let clerks handwrite SSN on checks as ID
- Don't have SSN preprinted on checks (re-order them without SSN)

## **Tips to Protect Yourself**

- Check your credit report annually (FACT Act ensures one free report per year from each of the three credit bureaus)
- Review all statements; check for unauthorized charges or suspicious activity
- Pick up new checks at the credit union
- Mail bills from a locked mailbox or Post Office
- Beware of shoulder surfers at ATMs
- Shred (with cross-cut shredder) pre-approved credit card offers, statements/bills with account numbers, and other documents before discarding them

## **More Tips. . .**

- Use electronic deposit of paychecks, dividends, pension and Social Security payments, and tax refunds
- Don't authorize payment over the phone unless you call a specific/known creditor
- Keep a list—in a safe place—of credit/share draft account numbers, expiration dates, and phone numbers to report theft

## **Know When You Have to Give SSN and When You Don't**

### **Must give SSN**

Credit unions/banks  
Employers  
Income tax records  
Vehicle registration  
Credit bureau reports  
College records  
Loan applications

### **May want to refuse**

Over the phone  
On personal checks  
On driver's license  
On club membership  
As ID for store purchases  
As general identification

## Spamming, Spoofing, and Phishing

*Spamming*—Sending unsolicited e-mail indiscriminately to multiple mailing lists, individuals, or newsgroups

*Spoofing*—Creating a replica of a legitimate Web page to fool you into submitting personal, financial, or password data

*Phishing*—Luring victims to a fake Web site through spam. See current scams at [antiphishing.org](http://antiphishing.org)

## **It's Probably a Phishing Attack!**

Beware e-mail messages that:

- Use a generic greeting (“Dear Visa customers” or “Dear friend”)
- Refer to an urgent problem
- State that your account will be shut down unless you reconfirm your billing information
- Urge you to click on a link within a message you weren't expecting
- Hughes Federal Credit Union will never email or call you to request member private or account information. Please notify us immediately at 520-794-8341 if you are suspect a phishing attempt or fraudulent caller.

## **Tips to Protect Yourself from Phishing Attacks**

- Don't click on links within e-mail messages you weren't expecting. Contact the company directly using its phone/Web address.
- Avoid e-mailing personal and financial information.
- Review all statements for unauthorized charges. If statement is late, call the credit union or credit card company.
- Report suspicious activity to the FTC. Send spam to: [spam@uce.gov](mailto:spam@uce.gov). File complaints at [ftc.gov](http://ftc.gov).

## **Protect your Computer**

- Install and update current virus software
- Install firewall software to partially guard against spyware
- To see if computer is infected with spyware, install spyware detection and removal software (such as Spybot Search and Destroy, or Ad-aware)
- Install a spam blocker, free from [antiphishing.org](http://antiphishing.org)
- Use a secure browser—it scrambles information you send over the Internet

## More Tips to Protect your Computer

- Don't download files or open attachments from strangers
- Only open attachments you're expecting
- Don't click on links from unfamiliar senders
- Use strong passwords—combination of letters (upper and lower case), numbers, and symbols
- Avoid automatic log-in; always log off when done
- Securely erase your hard drive before disposing of your computer:
  - Re-format hard drive (reinstall Windows), or
  - Use hard drive erase utility

## **Shop Safely Online**

- Shop only with companies you know
- Use secure browser (look for closed padlock or unbroken key at bottom of browser window—not payment page)
- Pay only with credit card, or with third-party intermediary (you have some protections if merchandise is defective, not as described, or is not received at all)
- Consider using a separate credit card for online purchases, to track purchases easily

## **Warning Signs You May be a Victim**

- Oftentimes, there aren't any!
- Your monthly credit card or financial statements contain fraudulent charges, or suddenly stop arriving
- You don't receive any mail for several days
- You are denied credit for no apparent reason
- You start getting bills from unfamiliar companies for goods or services you didn't request
- Credit collection agencies try to collect on debts that don't belong to you

## **No Warning Signs?**

- Check your credit report anyway!
- Get one free report per year from each bureau
  - [www.annualcreditreport.com](http://www.annualcreditreport.com)
  - 1-877-322-8228
- Look for accounts you didn't authorize
- Check for accuracy; dispute inaccuracies
- Beware of e-mails and Web sites offering "free" credit reports
- Don't give your SSN just to get a free report

## **If you're a Victim of ID theft...**

1. Contact one fraud unit (mandatory sharing among all credit bureaus, per FACT Act). Fraud alert will be placed on each of your credit reports within 24 hours.
2. Contact FTC's ID Theft Hotline at 877-IDTHEFT to speak with a counselor and report ID theft.
3. Contact each creditor (credit card companies, mortgage lender, credit union), and Social Security Administration to notify them of the fraud. Close all affected accounts. Follow each conversation with a letter and keep a copy. The FTC's "ID theft affidavit" simplifies the process. Go to [ftc.gov/idtheft](http://ftc.gov/idtheft).
4. File a report with local police department, and law enforcement agency where ID theft took place.
5. Get copies of police reports and send to all creditors.
6. Contact your financial institution immediately.

## The "Big Three" Credit Reporting Agencies

Experian

Order report: 888-397-3742

Fraud Unit: 888-397-3742

[experian.com](http://experian.com)

TransUnion

Order report: 800-888-4213

Fraud Unit: 800-680-7289

[transunion.com](http://transunion.com)

Equifax

Order report: 800-685-1111

Fraud Unit: 800-525-6285

[equifax.com](http://equifax.com)

Or use the central site  
sponsored by the 3 consumer  
reporting agencies:

[www.annualcreditreport.com](http://www.annualcreditreport.com)

## **Resources-**

- Call HFCU for copies of informative booklets
  - Beth McClure-Training Manager
  - (520) 205-5674
  - Or, email your request via our website  
(attention: Training/Education Department)
- [www.hughesfcu.org](http://www.hughesfcu.org)
  - Click on 'Email Us' icon at bottom of screen

## More Resources...

Federal Trade Commission  
CRC-240

Washington, D.C. 20580

877-IDTHEFT (toll-free)

[www.consumer.gov/idtheft](http://www.consumer.gov/idtheft)

Privacy Rights Clearinghouse

[privacyrights.org](http://privacyrights.org)

Better Business Bureau

[bbbonline.org](http://bbbonline.org)

National Do Not Call Registry

[www.donotcall.gov](http://www.donotcall.gov)

1-888-382-1222

# Hughes Federal Credit Union

*Yours for the Asking*

Remember...your credit union can help you with all your financial challenges.

