



ISSUE #13 – Q3 2005

- Time to Refresh – Protection Tips
- Universities – A Target for Thefts

TIME TO REFRESH – Protection Tips

Enough victims contacting Identity Fraud, Inc. could have prevented identity theft by taking some simple precautions. We refresh some useful protection tips as follows:

1. **Unsolicited Requests for Information:** Never give out your social security number, credit card info, or other personal information to someone that initiates contact with you.
2. **Phishing:** Never give out personal information in an online transaction that you did not initiate. Your Bank or Financial Institution will never email you confirmation of information they already have.
3. **Ask Questions:** You do not always need to give out your social security number when asked. If your state uses your social security number on your driver's license, request to have it changed to another number. If a business asks for your social security number ask the following questions and then decide if it
 - Why do you need my Social Security number?
 - How will my Social Security number be used?
 - How do you protect my Social Security number from being stolen?
 - What will happen if I don't give you my Social Security number?
4. **Out of Sight:** Never leave your credit card, Driver's License, social security card, or other document containing personal information out in the open for others to see. They can memorize it, copy it down, or even take a picture of it with a camera phone.
5. **Mail Fraud:** Instead of leaving bills to be mailed in your mailbox for the mailman to pick up, bring them directly to a secure mailbox location to be mailed. An identity thief can otherwise steal the mail right out of your mailbox. With one stolen credit card bill to be paid an identity thief could walk away with your credit card number, full name and billing address, your checking account number, and in some cases your Driver's License number if it is listed on your check.
6. **Password Protect:** Pick different levels of passwords for different levels of security, from simple passwords where no personal information can be obtained, to more complex passwords for banking purposes. For complex passwords especially, do not choose things that would be easy to guess, like a last name, birth date, or child's name. It is more secure to choose a random password made up of both letters and numbers.

Obtain Your Free Credit Report(s) –

Under the FACT Act (Fair and Accurate Credit Transactions Act of 2003), you are eligible to receive one free credit report per year from each main credit reporting agency, Equifax, Experian, and TransUnion.

You should review your credit reports for a) accuracy, and b) possible fraud.

Simply visit www.annualcreditreport.com or call 1-877-322-8228 for more details.

(Not currently available in all States, see web site for more details on availability).

7. **Credit Reports:** Take advantage of your right to one free credit report per credit bureau each year. Go to www.annualcreditreport.com and space out your reports every three months to maximize your awareness. Correct any inaccuracies and make sure nothing is on your credit report that may be an indication of identity fraud.

8. **Fraud Alerts:** Place verbal fraud alerts on your credit report by calling any one of the credit reporting agencies:

- **Equifax** **1-800-525-6285**
- **Experian** **1-888-397-3742**
- **TransUnion** **1-800-680-7289**

This alert can prevent new accounts from being opened in your name, by requesting the company looking to issue credit to call you at home first to verify your identity. These alerts are only good for 90 days, but as a reminder to set them you can do them at the same time you check your next free credit report.

Identity Theft Risk at Universities

Are you at risk?

Despite their image as leafy enclaves of higher learning shielded from the real world, universities across the United States are finding themselves on the front lines of the battle against identity theft. With their huge databases, universities may rival financial institutions as attractive targets for the crime, estimated to affect over 9 million Americans a year at the total cost of more than \$50 billion.

Nearly half of the publicized incidents of data breach since January occurred at universities. In academia, major institutions like the University of California system and smaller private schools from Tufts to Stanford are equally affected as hackers exploit computer vulnerabilities to access sensitive data and as laptops get stolen.

Protection through change and awareness...

The awareness of campus identity theft in California is partially a result of the 2003 state law requiring notification by state and public entities if an unauthorized third party acquires personal data. A bill by California Senator Dianne Feinstein to enact similar national legislation is one of many working their way through Washington. Another California state law forbidding the public posting of social security numbers has led more schools to scrap the common practice of using them as student identifiers.

The University of California has also gone beyond hardening its network to educating users on the dangers of keeping unencrypted files containing sensitive data on their computers and the vital need to maintain security patches.

