Los Angeles Community College District
Interoffice Memorandum

HUMAN RESOURCES DIVISION

Date: September 19, 2006

To: All District Employees

From: Michael Shanahan
Associate Vice Chancellor
Employer-Employee Relations

Re: **IDENTITY THEFT**

What You Can Do.

You should monitor your credit card statements and bank records to quickly identify any unfamiliar transactions.

Enclosed are several articles defining identity theft and offering suggestions to avoid or recover from identity theft. Read them carefully and heed their warnings.

If you believe you have been a victim of identity theft, follow the instructions to contact the credit reporting agencies and other institutions as soon as possible to minimize any damage to or disruption of your credit history.

Report possible incidents of identity theft to law enforcement, and specifically to your college deputy sheriff.

Identity Theft 101

Identity theft is a crime that involves someone else using your name, Social Security number and/or other personal information to steal. The theft can involve the use of your existing credit cards to purchase expensive items, opening new credit accounts in your name, making purchases or cash advances, or draining your financial accounts. Identity theft can even allow someone to use your name when arrested for criminal acts!

When a thief steals your wallet, you can take immediate action to protect yourself - call the police, notify your bank and credit union, and cancel credit card accounts. But with identity theft, you often are unaware of the crime for weeks or months, which gives the thief plenty of opportunities to do a lot of damage.

…with identity theft, you are often unaware of the crime for weeks or months…

There are two types of identity theft: *application fraud* and *account takeover*.

"Application fraud" is also known as "true name fraud." The identity thief uses your Social Security number or other personal information to open *new* accounts in your name. You may not become aware of this type of theft for months, because credit card account statements are mailed to the thief's address, not yours. However, victims of the other type of ID theft, called "account takeover," may learn of the crime as soon as they receive their next monthly account statement.

Frequently, your personal information is obtained through **"phishing"** email. Watch out for emails or calls that appear to be from a company you do business with, asking you to "verify" personal or account information.

"Account takeover" is the act of someone using your *existing* credit account information to purchase items using your actual card, or possibly just the account number and expiration date.

How could **your** identity be stolen? In addition to outright theft of your wallet or purse, these are the most common ways thieves could get access to your information:

- Obtaining your name, address, credit card or other account numbers by going through your mail or trash. Finding preapproved credit card offers is an easy way for the thief to cash in on your identity.

- Buying your credit information from an unscrupulous employee of a business you deal with. Most popular are auto dealerships and retail stores.

- Posing as a potential employer or landlord to order a copy of your credit report.

- Filing a change of address form to redirect your mail to a new address.

Once this information is in the hands of an identity thief, they can start stealing from you almost immediately. The theft can occur in one or more of these ways:

- Transferring money out of your financial accounts.

- Using your existing credit card to buy luxury items.

- Opening new credit accounts in your name.

- Renting an apartment and setting up utilities in your name.

- Setting up cell phone service in your name.

- Opening new checking or money market accounts in your name and writing bad checks.

- Changing the address on existing cards so you won't see the charges being made.

More than nine million people were victims of identity theft last year. Identity theft is a serious and growing phenomenon - it is the number one concern of people contacting the Federal Trade Commission. In a recent survey conducted by the Better Business Bureau, 9.3 million people were victims of identity theft in 2005 and the average amount of fraud per victim rose to $6,383.

9.3 million people were victims of identity theft in 2005.

Once discovered, it can take months to correct the damage done. In addition to notifying each financial account impacted, you must make sure that your credit report is updated. Otherwise, you could be denied credit next time you want to buy a home or a car. According to the FTC Identity Theft Survey of September 2003, less then 40% of identity theft victims contact the credit bureaus to report the incident!

Stay alert to illegal use of *your* personal information. Checking your credit report each year is a smart step to take in the on-going battle to protect your identity.

The Fair and Accurate Credit Transaction Act (FACTA) allows for all consumers to receive a free copy of their credit report from each of the three credit reporting bureaus every 12 months. Reports can be ordered through **annualcreditreport.com**.

How to Survive Identity Theft

When you are the victim of identity theft, you must deal with the logistical impact of the crime (contacting creditors, correcting your credit report, etc) as well as the emotional aftermath. The process may leave you feeling violated, frustrated and helpless. The following information can help you to figure out what to do if it happens to you. Knowing what to do and those to contact can empower you to get your credit straightened out and help you to regain your emotional balance.

What You Need to Know

Many identity theft victims have no idea what their rights are, and may make mistakes as a result. Here are five important facts to know before you make a move:

1. Federal law states that the victim of identity theft is liable for only the first $50 of losses if you notify the financial institution within two days of learning of the loss. Many financial institutions will waive even that amount.

2. You're entitled by law to a free copy of your credit report if you are a victim of identity theft.

3. You should not pay for items fraudulently purchased with your credit card. Stand by your legal rights. If you pay these bills, you are implying that you are responsible for the debts.

…Federal law states that the victim of identity theft is liable for only the first $50 of losses…

4. In most cases, do NOT change your Social Security number. Such a move makes you look *more* suspicious to future creditors, not less. And, it doesn't protect you from someone stealing the new number as well.

5. Explain the problem to collection companies and don't take harassment. If collection companies harass you after you have written to explain you were the victim of fraud, they could be violating federal law. Document such attempts and let them know you may take legal action if they continue.

What You Need to Do

Now that you know the ropes, it's time to take action. Contact the organizations listed below that apply to your situation:

Contact the police, especially if your wallet (or purse) was stolen. It's smart to notify the authorities of *any* identity theft crime, since it may be helpful to have a police report to back up your claims with creditors.

Contact the credit bureaus. This is an essential step for any victim of identity theft. There are two actions you should request:

- **Ask for a fraud alert** to be placed on your file.
- **Order a copy of your credit report** to see what fraudulent accounts may have been opened in your name.

The Fair and Accurate Credit Transaction Act (FACTA) allows for all consumers to receive a free copy of their credit report from each of the three credit reporting bureaus (*Equifax, Experian,* and *TransUnion*) every 12 months. Reports can be ordered through ***annualcreditreport.com*** or by calling **877-322-8228**. You will not be able to receive a free report by contacting the credit bureaus directly.

Contact your bank, credit union and creditors to let them know of your situation. Request an account freeze for any affected accounts.

Contact the Federal Trade Commission (FTC) to file a complaint. The Federal Trade Commission (FTC) maintains a toll-free identity theft hotline at 877-ID-THEFT (438-4338). Use their Identity Theft Affidavit to report your situation to the creditor of each new fraudulent account.

Contact the Postal Inspector if you suspect that someone has changed your address with the post office or used the mail to commit identity theft.

Contact Social Security to alert them to someone using your Social Security number. Their Fraud Hotline can be reached at 800-269-0271.

Contact your Department of Motor Vehicles if your driver's license number was used by a thief. They may recommend that you cancel the old number and receive a new one.

Surviving identity theft is never easy. But the information above should give you the tools you need to get through the worst of it.

Recovering From Identity Theft

The aftermath of identity theft can be as simple as a few calls to the credit bureaus or it can become a complicated nightmare that takes years to end. You can follow all the rules for reporting the crime and contacting creditors, but sometimes the problems just won't go away.

Victims of identity theft may get little help from authorities, who don't always have the resources to investigate these cases. With millions of cases reported each year, police and other agencies rarely get involved unless your case amounts to an exceptionally large theft.

Your first move towards recovery should be to arm yourself with the following documentation:

- The police report filed when you learned of the identity theft.
- An Identity Theft Affidavit to report the crime to your creditors.
- Copies of your credit report.
- Documentation from creditors, such as copies of the credit application filled out by the thief.

Another smart step is to file a report with the FTC's Identity Theft Hotline by calling **1-877-IDTHEFT (1-877-438-4338)**. Also, be sure to place a fraud alert with each of the three major credit bureaus (*TransUnion*, *Equifax* and *Experian*). While this is designed to alert lenders to contact you before issuing new credit in your name, it doesn't always work. Some lenders ignore the alert, and new accounts may continue to be opened by the criminal.

...be sure to place a fraud alert with each of the three major credit bureaus.

Finally, request that all of your existing creditors code your accounts so that a password you select is required before changing the address, increasing your credit limit, etc. Make sure to keep a log of all your efforts - write down the date and time, whom you spoke and what was discussed.

Some victims must also deal with abusive collection agencies that refuse to believe that someone else incurred the debt. Instead of getting assistance with the problem, they may be threatened with lawsuits and garnished wages. To combat this problem if it happens to you, send a copy of the police report. If one is not available, demand that they send you proof of the debt (which is required under The Fair Debt Collections Act). Once you receive this, you'll be able to demonstrate that the signature, address, etc. are not yours, and that therefore you are not responsible for the debt.

There are certain things you should definitely **not** do when trying to resolve your identity theft crisis:

- Do not pay any bill or debt that is a result of fraud.
- Do not cover any checks that were written or cashed fraudulently.
- Do not file for bankruptcy without consulting with a professional.
- Do not change your Social Security number (unless advised to do so by Social Security - a rare occurrence).
- Do not be intimidated into paying any debt that you did not incur.

Do not be intimidated into paying any debt that you did not incur.

Going through identity theft recovery is emotionally draining. Many victims suffer symptoms similar to those of survivors of assault or other serious crimes. You may feel both helplessness and rage at your situation, as well as loss of financial security.

Seek counseling if necessary to help you cope with these feelings and try to find local support groups so you can talk to others that have been through the same experience.

Almost 30% of online consumers have not made a purchase because they are worried about privacy issues.

Protecting Your Identity Online

Just ten years ago, most of us couldn't conceive of buying items online. The biggest concern was privacy - if we entered our credit card information to make a purchase, we worried that a “hacker” would steal it and go on a spending spree.

Since the introduction of encryption software, most web sites can offer assurances that your credit card information is safe. Encryption scrambles the information you send, such as your credit card number, so that anyone without legitimate access can't misuse the data. And of course, you have the same protection with online purchases as with any others - the Fair Credit Billing Act limits your responsibility for fraudulent credit card purchases to $50.

Online Shopping on the Rise

According to the e-tailing group, in 2005 ecommerce reached $172 billion, up 47% from $117 billion in 2004. Much of the increase is due to the popularity of online auction sites, such as EBay and Yahoo Auctions as well as retailers such as Amazon.com and Wal-Mart.

The following tips can help you to feel comfortable shopping online:

- The same advice for avoiding low-tech identity theft applies to shopping on the Internet - know who you are dealing with and don't supply information that can be misused, such as your Social Security number.

Never send your credit card information for payment by email.

- Never send your credit card information for payment by email - since there is no security protection.

- Read the website's privacy and security policies page - it will let you know what encryption methods are in place and whether they share your information with any third parties or affiliates.

- Only buy from secure websites. You can tell if the URL of the order page is secure because it has “https” in the address, rather than “http.” It's actually more secure to use your credit card online than giving out your credit card number over the phone for a catalog purchase.

- Use a credit card rather than a debit card, since debit cards are not protected by federal law to the same extent as credit cards.

- When paying for online auctions, consider using an “e-payment” service such as PayPal. They allow you to pay any seller with your credit card without providing your credit card information to an unknown party.

Other Online Usage

Whether you're browsing for information, registering for a chat site or subscribing to a magazine, you may often find yourself needing to enter personal information. How can you be sure that someone won't misuse that info?

Some of the steps you can take are the same as those for shopping online - check the website's privacy policy and security, and provide only essential information. Here are some other tips that can keep your identity safe:

- **Keep your passwords private** - don't ever give any passwords to a stranger, no matter what the circumstances. And change your passwords often to protect yourself from hackers.

- Don't fall for emails or pop-up ads which announce, “You have won” a free prize or sweepstakes. At best, they will be sales come-ons, at worst an attempt to snag your credit card or other identifying information.

- Be cautious about online offers for credit cards; many of these are fraudulent while others are hyping cards with expensive fees and interest rates.

- You may find your email inbox flooded with emails promising everything from credit repair and free scholarships to lucrative work-from-home businesses. Just delete these, since most are outright scams.

Using these tips will definitely help to keep your identity safe while using the power of the World Wide Web.