

# CONCERN EMPLOYEE ASSISTANCE PROGRAM

A Benefit for Employees  
and Families



CONCERN:EAP

# CONCERN: EAP SERVICES

- Work/Life Benefits
  - Parenting & Childcare Resources
  - Older Adult Services
  - Financial Counseling
  - Legal Consultations
  - Career Management
- Short-term Counseling visits per issue per 12-month period
- Free, Confidential -- 24/7 800 number answered "live"



CONCERN:EAP

# Getting Started

- Call for an appointment 6:30 a.m. - 5:00 p.m. (Pacific Time) Monday through Friday
- In crisis situations, call 24/7 for immediate telephone support
- For more information:
  - ask your HR/Benefits Department
  - [www.concern-eap.com](http://www.concern-eap.com)
  - call CONCERN at (800) 344-4222



# **CLC, Incorporated**

Presents

## **Identity Theft: Prevention and Resolution**

*“One out of every five Americans, or a member of their family has been victimized by identity theft.”*

## The Identity Theft Crisis

- The FTC states that identity theft is one of the fastest growing crimes in the nation. One out of every five Americans, or a member of their family have been victimized by identity theft.
- Identity theft complaints nearly doubled in 2003 and has topped the government's list of consumer frauds for a third consecutive year.
- The Identity Theft Resource Center reports fraudulent charges now average more than \$90,000 per identity stolen.



## The Need for ID Theft Assistance

- Identity theft is a crime that is almost solely on the shoulders of the victim to resolve. Currently there is little assistance given to consumers who need to resolve ID theft issues.
- The average consumer spends over 175 hours and over \$1,500 per occurrence resolving ID theft issues.
- It will take a victim of ID theft an average of 2 to 5 years to clear-up resulting credit related problems.
- If a consumer does not respond to a creditor within 2 weeks of identity theft their chances of recovery are greatly decreased.

## How Identity Theft Occurs

*"I was first notified that someone had used my Social Security number for their taxes in February 2004. I also found out that this person opened a checking account, cable and utility accounts and a cell phone account in my name. I'm still trying to clear up everything and just received my income tax refund after waiting four to five months. Trying to work and get this all cleared up is very stressful"*

*From a consumers complaint to the FTC, July 9, 2004*

## How Bad People Get Good Credit!

*It's so easy for your information  
to get into the wrong hands*

- Shoulder surfing and dumpster diving
- Phishing and skimming
- Insider interloping or impostor access
- Stealing wallets & mail mulling
- Diverting your mail
- Internet intruding
- Posing as your employer or creditor to obtain a copy of your credit report
- Using credit card slips left at restaurants or not properly destroyed
- Stealing and completing "pre-approved" credit card offers



## HEADLINES

- **April 13, 2004 — Navy, Police Investigate Identity Theft Ring Suspects Allegedly Used Personal Information To Open Charge Accounts — *Quest Diagnostics***
- **March 9, 2005 — customer data used in fraud. The Company's parent firm suspects a hacker stole the information. — *DSW Shoe***
- **March 9, 2005 U.S. Citizens' Data Possibly Compromised — *Lexis-Nexus***
- **March 11, 2005 — Senators rip into *ChoicePoint, Bank of America* on data losses.**
- **March 28, 2005 — Stolen Laptop Exposes Data of 100,000 — *University of CA***

## How Identity Thieves Use Your Personal Information

- Call your credit card issuer to change the billing address.
- Open new accounts in your name.
- Establish phone or wireless accounts in your name.
- Open a new bank account and write bad checks on that account.
- Counterfeit checks or debit cards or authorize electronic transfers in your name and drain your bank account.
- File bankruptcy under your name to avoid paying debts.
- Buy a car by taking out a loan in your name.
- Get a driver's license issued with their picture and your name.
- Get a job or file fraudulent tax returns in your name.
- Give your name to the police during an arrest.

## Some Easy Tips On Ways To Protect Yourself from Identity Theft

- DO NOT CARRY your Social Security card, birth certificate or passport in your wallet.
- If you have multiple credit cards, don't carry all of them.
- When you pay your bills, do not leave them in your mailbox for the mail carrier to collect.
- When you order new checks, pick them up at your your bank so they do not have to be mailed to you.
- If you can, install a locked mailbox at your home to deter mail theft.
- Make a detailed inventory or photocopy all your credit cards, bank accounts and investments: account numbers, expiration dates & telephone numbers of the company.

## Some Easy Tips On Ways To Protect Yourself from Identity Theft

- If you are going to be away from home more than two days, always have your mail held at the Post Office or ask a trusted friend to pick it up.
- Unless you initiate the call, *NEVER* provide anyone with your personal information over the phone.
- When paying with a credit card always take the copy of the receipt with you. *NEVER* toss it in a public trash container and if shopping, put receipts in your wallet rather in the shopping bag.
- When creating password and personal identification numbers (PINS) do not use the last four digits of your Social Security number, mother's maiden name, birth date, middle name, pet's name, consecutive numbers or anything else that could be easily discovered by thieves.
- Create passwords that combine letters and numbers.
- Never write down your PIN(s) on the card or carry them in your wallet.

## Some Easy Tips On Ways To Protect Yourself from Identity Theft

- Use hand, arm or elbow to shield when using your PIN at an ATM machine, debit machine in a retail store or when using your phone calling card.
- Always protect your Social Security Number and give it out only when absolutely necessary (tax forms, employment records, most banking, stock and property transactions).
- Examine your Social Security Personal Earnings and Benefits Estimate Statement each year to check for fraud.
- If anyone is using your Social Security number as an identification number (State Motor Vehicle Administrations, medical benefit companies) contact them and request a different number.
- Do not toss "pre approved" credit card offers in your trash or recycling bin without first tearing/shredding them into small pieces. They can be used by dumpster divers.
- Buy a shredder and always shred sensitive documents.

## Some Easy Tips On Ways To Protect Yourself from Identity Theft

### Internet & Computer Security

- When purchasing on the Internet, always make certain the site is a "secure site" and use your credit card, not your debit card.
- Install a firewall on your home computer to prevent hackers from obtaining personal identifying and financial data from your computer's hard drive. This is especially important if you connect through a cable or DSL company.
- Delete any personal information stored on your computer before you dispose of it. Use a "wipe" utility program that makes files unrecoverable.
- On your laptop avoid using an automatic log-in feature and always log off. If stolen -- a thief will have a hard time accessing the information.

## Some Easy Tips On Ways To Protect Yourself from Identity Theft

- Try not to store financial information on your laptop. If you do, use a “strong” password – that is a combination of letters (upper and lower case), numbers and symbols. Ex: Md19J%2
- Don’t download files from strangers or click on hyperlinks from people you don’t know.
- Always take your computerized hotel room key with you and destroy it or turn it back into the hotel desk as some hotels input credit info on the cards.

“For example, if you have done your tax return online and have saved it in your computer, and your child is online sharing music, and the default is to share whatever is on your computer, your tax return information which includes your social security number and all your other pertinent information could be shared.”

***March 23, 2005 – Lisa Hicks-Thomas, Chief of the Attorney General's Computer Crime Unit - Virginia***

## Some Easy Tips On Ways To Protect Yourself from Identity Theft

### Reducing Vulnerability at Work

- Don't leave or store sensitive personal information in your office (Benefit Statements, 401 (k) information) unless in a locked drawer.
- Don't store personal information on your desktop computer.
- Don't print sensitive information unless the printer is close at hand.
- Don't leave negotiable instruments such as checks at work.
- NEVER leave your purse unattended.
- Don't use your Social Security as employees IDS
- Ask if your business locks personnel files when not in use.
- See who is within earshot of a sensitive conversation – when you order merchandise over the phone and you give your credit card number.
- Don't put your bills, checks, or other correspondence in an unguarded outgoing mail slot.



# ID Theft Emergency Response Protocol

## Immediate Steps To Follow

1. Make a Police Report and obtain a copy.
2. Notify the fraud departments of all creditors.
3. Place a Fraud Alert on your Credit Report.
4. Review your Credit Report at the end of the 90 day period.
5. Report the fraudulent activity to the authorities (USPS, MVA) and forward this report to all creditors.
6. Close any account you know or believe has been tampered with or opened fraudulently.
7. Ask for contact info from the individual you are reporting your fraudulent case.
8. Always keep copies of any correspondence/forms.
9. Keep old files even though you believe the case is closed.
10. Report the ID Theft to the Federal Trade Commission.
11. Individuals may want/need support from a qualified Identity Theft Response program.