

Credit Card Management Services, Inc.

Quarterly Newsletter April 2004

Volume 2

A Non-Profit Company

Issue 2

Identity Theft

In the course of a busy day, you may write a check at the grocery store, charge tickets to a ball game, rent a car, mail your tax returns, call home on your cell phone, you'd like to know more about protecting yourself from order new checks or apply for a credit card. Chances are this devastating crime. you don't give these everyday transactions a second thought. But someone else may.

The 1990's spawned a new variety of crooks called identity thieves. Their stock in trade is your everyday transactions. Each transaction requires you to share personal information: your bank and credit card account numbers, your income, your Social Security number (SSN), or your name, address and phone numbers. An identity thief co-opts some piece of your personal information and appropriates it without your knowledge to commit fraud or theft. An all-too-common example is when an identity thief uses your personal information to open a credit card account in your name.

Identity theft is a serious crime. People whose identities have been stolen can spend months or years — and thousands of dollars — cleaning up the mess the thieves have made of their good name and credit record. In the meantime, victims may lose job opportunities, be refused loans for education, housing, cars, or even be arrested for crimes they didn't commit. Humiliation, anger and frustration are common feelings victims experience as they navigate the arduous process of reclaiming their identity.

Perhaps you've received your first call from a collections agent demanding payment on a loan you never took out — for a car you never bought. Maybe you've already spent a significant amount of time and money calling financial institutions, canceling accounts, struggling to regain your good name and credit. Or maybe

your wallet's been stolen, or you've just heard about identity theft for the first time on the nightly news, and

The Federal Trade Commission (FTC), working with other government agencies and organizations, has produced this information to help you guard against and recover from identity theft. Can you completely prevent identity theft from occurring? Probably not, especially if someone is determined to commit the crime. But you can minimize your risk by managing your personal information wisely and cautiously.

If you've been a victim of identity theft, call the FTC's Identity Theft Hotline toll-free at 1-877-IDTHEFT (438-4338). Counselors will take your complaint and advise you on how to deal with the credit-related problems that could result. In addition, the FTC, in conjunction with banks, credit grantors and consumer advocates, has developed the ID Theft Affidavit to help victims of ID theft restore their good names. The ID Theft Affidavit, a form that can be used to report information to many organizations, simplifies the process of disputing charges with companies where a new account was opened in your name. For a copy of the ID Theft Affidavit visit the ID Theft website at www.consumer.gov/ idtheft.

The Hotline and website give you one place to report the theft to the federal government and receive helpful information. The FTC puts your information into a secure consumer fraud database where it can be used to help other law enforcement agencies and private entities in their investigations and victim assistance.

Credit Card Management Services, Inc. 4611 Okeechobee Blvd. Suite 114 West Palm Beach. FL 33417 Phone: 1-800-920-2262 Fax: 1-866-561-2622 Web: www.debthelper.com

The information contained in this month's newsletter was provided by the Federal Trade Commission (www.ftc.gov) in their publication "ID Theft: When Bad Things Happen to Your Good Name." To receive a copy of the full publication or other helpful FTC publications, please visit the FTC website at www.ftc.gov/bcp/menu-credit.htm or call 1-877-382-4357.

Page 2

Identity Theft - If You're a Victim...

Sometimes an identity thief can strike even if you've been very careful about keeping your personal information to yourself. If you suspect that your personal information has been hijacked and misappropriated to commit fraud or theft, take action immediately, and keep a record of your conversations and correspondence. Exactly which steps you should take to protect yourself depends on your circumstances and how your identity has been misused. However, four basic actions are appropriate in almost every case.

1. Place a fraud alert on your credit reports and review your credit reports.

Call the toll-free fraud number of any one of the three major credit bureaus to place a fraud alert on your credit report. This can help prevent an identity thief from opening additional accounts in your name. As soon as the credit bureau confirms your fraud alert, the other two credit bureaus will automatically be notified to place fraud alerts on your credit report, and all three reports will be sent to you free of charge.

- <u>Equifax</u> Call: 1-800-525-6285, and write: P.O. Box 740241, Atlanta, GA 30374-0241
- <u>Experian</u> Call: 1-888-397-3742, and write: P.O. Box 9532, Allen, TX 75013
- <u>TransUnion</u> Call: 1-800-680-7289, and write: Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790

Once you receive your reports, review them carefully. Look for inquiries you didn't initiate, accounts you didn't open, and unexplained debts on your true accounts. Where "inquiries" appear from the companies that opened the fraudulent accounts, request that these "inquiries" be removed from your report. You also should check that information such as your SSN, address, name or initial, and employers are correct. Inaccuracies in this information also may be due to typographical errors. Nevertheless, whether the inaccuracies are due to fraud or error, you should notify the credit bureau as soon as possible by telephone and in writing. You should continue to check your reports periodically, especially in the first year after you've discovered the theft, to make sure no new fraudulent activity has occurred. The automated "one-call" fraud alert process only works for the initial placement of your fraud alert. Orders for additional credit reports or renewals of your fraud alerts must be made separately at each of the three bureaus.

2. Close any accounts that have been tampered with or opened fraudulently.

Credit Accounts—Credit accounts include all accounts with banks, credit card companies and other lenders, and

phone companies, utilities, ISPs, and other service providers. If you're closing existing accounts and opening new ones, use new Personal Identification Numbers (PINs) and passwords. If there are fraudulent charges or debits, ask the company about the following forms for disputing those transactions: For new unauthorized accounts, ask if the company accepts the ID Theft Affidavit (available at www. ftc.gov/bcp/conline/pubs/credit/affidavit.pdf) or ask them to send you the company's fraud dispute forms. For your existing accounts, ask the representative to send you the company's fraud dispute forms. If your ATM card has been lost, stolen or otherwise compromised, cancel the card as soon as you can. Get a new card with a new PIN.

Checks—If your checks have been stolen or misused, close the account and ask your bank to notify the appropriate check verification service. While no federal law limits your losses if someone steals your checks and forges your signature, state laws may protect you. Most states hold the bank responsible for losses from a forged check, but they also require you to take reasonable care of your account. For example, you may be held responsible for the forgery if you fail to notify the bank in a timely way that a check was lost or stolen. Contact your state banking or consumer protection agency for more information. You also should contact these major check verification companies. Ask that retailers who use their databases not accept your checks.

- <u>TeleCheck</u> 1-800-710-9898 or 927-0188
- <u>Certegy, Inc</u>. 1-800-437-5120
- International Check Services 1-800-631-9656

Call SCAN (1-800-262-7771) to find out if the identity thief has been passing bad checks in your name.

3. File a report with your local police or the police in the community where the identity theft took place. Keep a copy of the report. You may need it to validate your claims to creditors. If you can't get a copy, at least get the report number.

4. File a complaint with the FTC.

By sharing your identity theft complaint with the FTC, you will provide important information that can help law enforcement officials track down identity thieves and stop them. The FTC also can refer victim complaints to other appropriate government agencies and companies for further action. To file a complaint or to learn more about the FTC's Privacy Policy, visit www.consumer.gov/idtheft. If you don't have access to the Internet, you can call the FTC's Identity Theft Hotline: toll-free 1-877-IDTHEFT; or write: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

Ms