LEWITT HACKMAN
LEWITT, HACKMAN, SHAPIRO, MARSHALL & HARLAN
A LAW CORPORATION
16633 VENTURA BOULEVARD, 11TH FLOOR • ENCINO, CALIFORNIA 91436
(818) 990-2120 • WWW.LEWITTHACKMAN.COM

IDENTITY THEFT NEWSLETTER

Judging from what we have observed recently through the media, it should come as no surprise that significant numbers of clients have contacted us seeking advice and help on identity theft. With the latest rash of security breaches, our clients are facing an attack on their personal and financial privacy unlike that faced by any prior generation. Because of the magnitude of the problem, Lewitt Hackman is providing the information in this newsletter to our friends and clients so they can guard against identity theft and take precautions to protect their personal and financial information.

ID theft is not new, but advances in technology and the growing sophistication of criminals have made it easier than ever. Because of the availability of credit and the ease of accessing personal information, it is easy for thieves to assume someone else's identity. With available software, identity thieves can use just one piece of stolen information to create full identification sets and forge Social Security cards, driver's licenses, and passports.

How do identity thieves get your personal information?

- They steal your wallet or purse.
- They rummage through your trash, the trash of businesses, or public trash dumps in a practice called "dumpster diving" to obtain bank and credit card statements, new checks and tax information.
- They retrieve credit card offers from your trash or mailbox and return them to the bank, requesting that the card be sent to an alternative address.
- They change your mailing address, so they can receive your mail.
- They read your personal identification number ("PIN") over your shoulder at an ATM.
- They send you unsolicited e-mail messages ("spam") that appear to come from legitimate businesses. These authentic-looking messages falsely indicate there is a problem with your account and ask you to provide account numbers and passwords to fix the error.
- They swipe your card through a $300 device called a "skimmer" during a legitimate transaction, e.g. at a restaurant or store. The information from the magnetic strip is stored in the "skimmer" and later used to create a duplicate credit card.
- They offer low interest rates on mortgages, congratulate you on being a contest winner or ask you to conduct a survey. When you answer, you give them personal information.
- They may pose as landlords, employers, or someone else with a legal right to access your credit report.
- They may steal personal information they find in your home.
- They may even photocopy your vital credit information legally at the courthouse. If you've been divorced, your financial and credit information may be part of the proceedings and are public record.

How do identity thieves use your personal information?

- They apply for credit cards in your name, often giving an address that is different from yours.
- They may buy a car or rent an apartment in your name.
- Some may even commit crimes in your name.
- They may counterfeit your checks or credit or debit cards, or authorize electronic transfers in your name and drain your bank account.
- They may have your driver's license issued with their picture.
- They may get a job or file fraudulent tax returns in your name.
- They may give your name to the police during an arrest. When they don't show up for court, an arrest warrant is issued in your name.
- They may file for bankruptcy using your name to avoid paying debts they've incurred or to avoid eviction.
- They may establish telephone or cellular service or utilities using your name.
- They may file a tax return using your name to obtain your refund.

How do you protect yourself?

- Destroy unnecessary personal records and statements. Buy a shredder and shred or tear up any documents that contain identifying information.
- Monitor your accounts. Order a copy of your credit report as often as possible, at least every six months.
- Don't carry important data in your wallet or purse.
- Keep financial information in a secure place in your home.
- Safeguard your Social Security number. Don't give it out to any person or company unless you are familiar with them and you have initiated the communication. Ask if you can use other identification.
- Shield your hand when entering your PIN at a bank ATM. The "shoulder surfers" are watching.
- Don't carry more credit cards than you really need.
- Pick up new checks or reissued credit cards at your bank.
- Empty your mailbox quickly, lock it or get a P.O. box so criminals don't have a chance to steal sensitive information.
- Never mail outgoing bill payments and checks from home. They can be stolen from your mailbox and the payee's name erased with solvents.

LEWITT HACKMAN
LEWITT, HACKMAN, SHAPIRO, MARSHALL & HARLAN
A LAW CORPORATION
16633 VENTURA BOULEVARD, 11TH FLOOR
ENCINO, CALIFORNIA 91436

- Do not give your credit card number or financial information over the internet unless you are certain you have a secure server connection. A secure website usually will display a "closed lock" or "key" at the bottom of the screen.
- Take your name off marketing lists. Call **1-888-5-OPTOUT** and ask that your name be removed from marketing lists. Ask financial firms not to trade your personal data.
- Do not do business online without reviewing the privacy policy of any on-line company.
- Install an electronic firewall on your computer to keep hackers from gaining access.
- Review your bank and credit card accounts carefully.
- Don't click on a hot link that seems to come from banks, brokerages, and online retailers.
- Alert your card issuer if you do not receive your statements. Someone may have taken them from your mailbox or changed the mailing address on your credit card.
- Do not use your mother's maiden name, your pets' name, your date of birth, or your middle name as a password. Don't write a pin number or social security number on anything you are going to discard (e.g. a receipt).

Steps to take if you are a victim.

- Place an initial fraud alert on your credit file. Contact any one of the three large credit rating agencies: Equifax **1-800-525-6285**, Experian **1-888-397-3742,** or Trans Union **1-800-680-7289**, and they will contact the other two. Ask to place a 90-day fraud alert and ask for a free copy of your credit report. Keep good records.
- Tell the police. Insist they make a report. Get a copy and number of the report. You'll need to file a police report if you want to: (a) have credibility with banks and other creditors; (b) extend your fraud alert for seven years, or (c) correct records. Include copies of your credit reports and communications with creditors. Be detailed.

We are experiencing an attack on our personal and financial privacy unlike that faced by any prior generation!

- Call the security departments of your credit-card issuers and other lenders. Follow up by sending certified letters that confirm details of your talks with the credit bureaus and the police. Request that you not be held responsible for fraudulent activity. Close accounts that have been tampered with and have the accounts marked "closed at consumer's request."
- Sign and notarize an identity theft affidavit. The FTC provides a format at **www.consumer.gov/idtheft.**
- Enclose copies of the ID theft affidavit and the police report with each certified letter to the creditors. Fill out the lenders' fraud forms if requested.

In the last several months, Lewitt Hackman has helped recover over $400,000 in assets for our clients that were all but lost as a result of identity theft. We want to ensure that our clients are protected and understand what is at stake.

Most identity theft victims put off hiring a lawyer until the sheriff is serving them with a summons. Bad decision. The time to retain counsel is before the banks and credit card companies are suing you. **Prevention is the key to protection!**

Having helped several victims of identity theft, we can tell you that identity theft crimes can have deep and lasting effects. Identity theft is not a battle you should wage alone.