

*Safeguarding your finances...  
your health...your good name*



# **IDENTITY THEFT TODAY**

- ➔ **Account Hijacking**
- ➔ **Credit Card Fraud**
- ➔ **Medical Identity Theft**
- ➔ **Early Detection Tips**

**IDENTITY THEFT IN ITS MANY FORMS CONTINUES TO BE A CONCERN...**one that your credit union and financial regulators are addressing daily. Identity theft occurs when someone steals your personal information to establish credit or borrow money in your name. It is important to remember, however, that just as our defenses against identity theft become more sophisticated, so too the methods criminals use to defraud consumers. Knowing the threat is the first line of defense, say the experts. That means keeping abreast of the frauds active in today's environment...and knowing what you can do to protect yourself.

## **ACCOUNT HIJACKING**

Recent studies indicate that unauthorized access to checking and share draft accounts is the fastest growing form of identity theft, occurring primarily through phishing and hacking.

**Hijacking by Phishing** occurs when a person provides personal information (social security number, account numbers, etc.) in response to a fraudulent email, often a ruse to correct a "problem" with your account.

**Hijacking by Spyware** can occur when malicious software (called malware) invades a computer and collects personal information for a criminal's use. The computer owner is usually unaware it is occurring.

### ***What You Can Do***

---

**Password**—Make it unique, and hard for criminals to guess (e.g., do not use your street address).

**Anti-Virus**—Keep your computer's anti-virus software up-to-date. New viruses are being created every day.

**Anti-Spyware**—Software to detect and remove spyware is readily available and should be on all computers.

**Don't Get Phished**—Don't answer any suspicious emails. And always remember that your credit union will not ask you to “verify” any information through an email. If you get such an email, it's a scam.

## **CREDIT CARD FRAUD**

Stolen credit card information is the most common transaction fraud. In its simplest form, it involves a criminal stealing your credit card information and running up charges in your name. Alternatively, fraudsters can steal personal information by phishing, spyware or other means, then open new credit card accounts in your name. Left unchecked, it can spoil your credit record, ruin your credit score, and make it difficult to land a new mortgage or even a job!

Regardless of the means, the result is that victims must spend extensive time and energy correcting the damage done by having credit charged illegally in their name.

## **BEWARE OF A GROWING FRAUD... MEDICAL IDENTITY THEFT**

Medical identity theft is a growing fraud that has substantial consequences on victims' well-being and can impact the victim financially. Victims of medical identity theft may experience the now-familiar consequences of financial identity theft, including

- loss of credit
- harassment by debt collectors and
- inability to find employment or get credit.

Medical identity theft occurs when someone uses a person's name and other personal information—such as insurance information—to

## ***What You Can Do***

---

- Implement the computer security measures noted with Account Hijacking.
- Destroy credit card solicitations before throwing them away. “Dumpster-diving” is still one of the ways criminals get cards in your name.
- Shred financial statements before discarding.
- Prepare a list of your credit card numbers and company contact information.
- Report lost or stolen cards immediately.

## **➔ IMPORTANCE OF EARLY DETECTION**

Regardless of the type of identity theft involved, some simple preventive measures can save you time and trouble, and perhaps ward off identity theft altogether.

## ***What You Can Do***

---

**Monitor Your Accounts Regularly**—People who monitor their accounts online tend to detect


obtain medical services or goods. It can lead to an inaccurate diagnosis of a condition and could be fatal if the information causes a drug interaction, allergic reaction or inappropriate diagnoses.

***What You Can Do:*** The Health Insurance Portability and Accountability Act (HIPAA), is a federal privacy act that protects patients from unauthorized access to personal medical information and addresses the problem of errors in medical records. Learn more at

**[www.hhs.gov](http://www.hhs.gov)**  
**[www.webmd.com](http://www.webmd.com)**  
**[www.privacyrights.org](http://www.privacyrights.org)**

## CHECK LIST FOR VICTIMS

If you become a victim of identity theft you should do the following:

-  File a police report.
-  Contact your credit union and cancel your credit cards.
-  Notify credit bureau fraud units.
-  Place a fraud alert statement on your credit report.
-  Request that credit bureaus identify accounts closed due to fraud as “closed at consumer’s request.”
-  Request a free credit report at **[www.annualcreditreport.com](http://www.annualcreditreport.com)**.
-  Report check theft to check verification companies.
-  Check post office for unauthorized change of address requests.
-  Follow-up telephone contacts with letters and keep copies of all correspondence.

hijacking earlier. In one report, victims' losses were a fraction of those who detected crime via paper statements.

**Check Your Credit Score**—Monitoring this important rating of your credit will often provide early detection of fraudulent activity, as well as provide the means to protect your accounts while you undertake further investigation. Federal law permits you one free credit report per year from each of the three major agencies. That means you can request one from each every 4 months.

**HOW TO OBTAIN A FREE CREDIT REPORT**  
**[www.annualcreditreport.com](http://www.annualcreditreport.com)**  
**(877) 322-8228**

Your credit union is taking substantive steps to protect your identity and make your financial transactions as safe and secure as they can be. This includes organization-wide evaluation of security systems, employee security training, and implementation of new online security measures. To learn more about these important benefits, contact your credit union.